



# **CERTIFIED PHA - HAZOP LEADER**

**TÜV SÜD Middle East**

**Add value.  
Inspire trust.**

# Disclaimer

- **Main source** for content [PHA-HAZOP Leader]: Regulation (EU) 2017/745 (a complete list of all referenced sources is provided in a reference list at the end)

## General information

Due to the constantly changing legal and legislative situation, we do not assume any guarantee with regard to up-to-date and legal bindingness. We are not liable for deviations from the content of the original documents. As far as laws and ordinances or other regulations are referred to or quoted, the official announcement is the only authoritative version.

Always keep yourself up to date on your own responsibility. To make the text easier to read, all references to persons apply equally to all genders. The pronouns used apply to all genders.





# Glossary



List of terms in a special subject, field, or area of usage, with accompanying definitions.

|      |                                  |                                                                                                                                                                                           |
|------|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BPCS | Basic Process Control System     | System which handles process control and monitoring for a facility or piece of equipment.                                                                                                 |
| DC   | Diagnostic Coverage              | an estimate of the proportion of failures that would be detected by the proof test or auto-test.                                                                                          |
| DCS  | Distributed Control System       | computerized system that automates industrial equipment used in continuous and batch processes, while reducing the risk to people and the environment.                                    |
| ESD  | Emergency Shutdown System        | An automatic protection system which will act to shut down the plant if it enters a potentially dangerous state.                                                                          |
| IPL  | Independent Protection Layer     | A device, system, or human action, which meets the core attributes to the necessary level of rigor and is capable of preventing an initiating cause from propagating to a hazardous event |
| PFD  | Probability of Failure in Demand | measure of the reliability of a Safety Instrumented Function (SIF) and represents the likelihood that the system will fail to perform its intended safety function when demanded.         |
| RRF  | Risk Reduction Factor            | the number of times that risk is reduced as a result of the application of a safeguard.                                                                                                   |
| SGS  | Safeguarding System              | Also Called ESD System or Logic Solver                                                                                                                                                    |
| SFF  | Safe Failure Fraction            | the fraction of the overall random hardware failure rate of a device that results in either a safe failure or a detected dangerous failure.                                               |

# CERTIFIED PHA - HAZOP LEADER

## INTRODUCTION



**01**

**Module 1**  
INTRODUCTION

**02**

**Module 2**  
PROCESS SAFETY MANAGEMENT

**03**

**Module 3**  
HAZOP

**04**

**Module 4**  
REHAZOP & LOPA

**05**

**Module 5**  
Checklists

**06**

**Module 6**  
WHAT IF & FMEA

**07**

**Module 7**  
LEADERSHIP

**08**

**Module 8**  
BOWTIE ANALYSIS



# 1

# INTRODUCTION

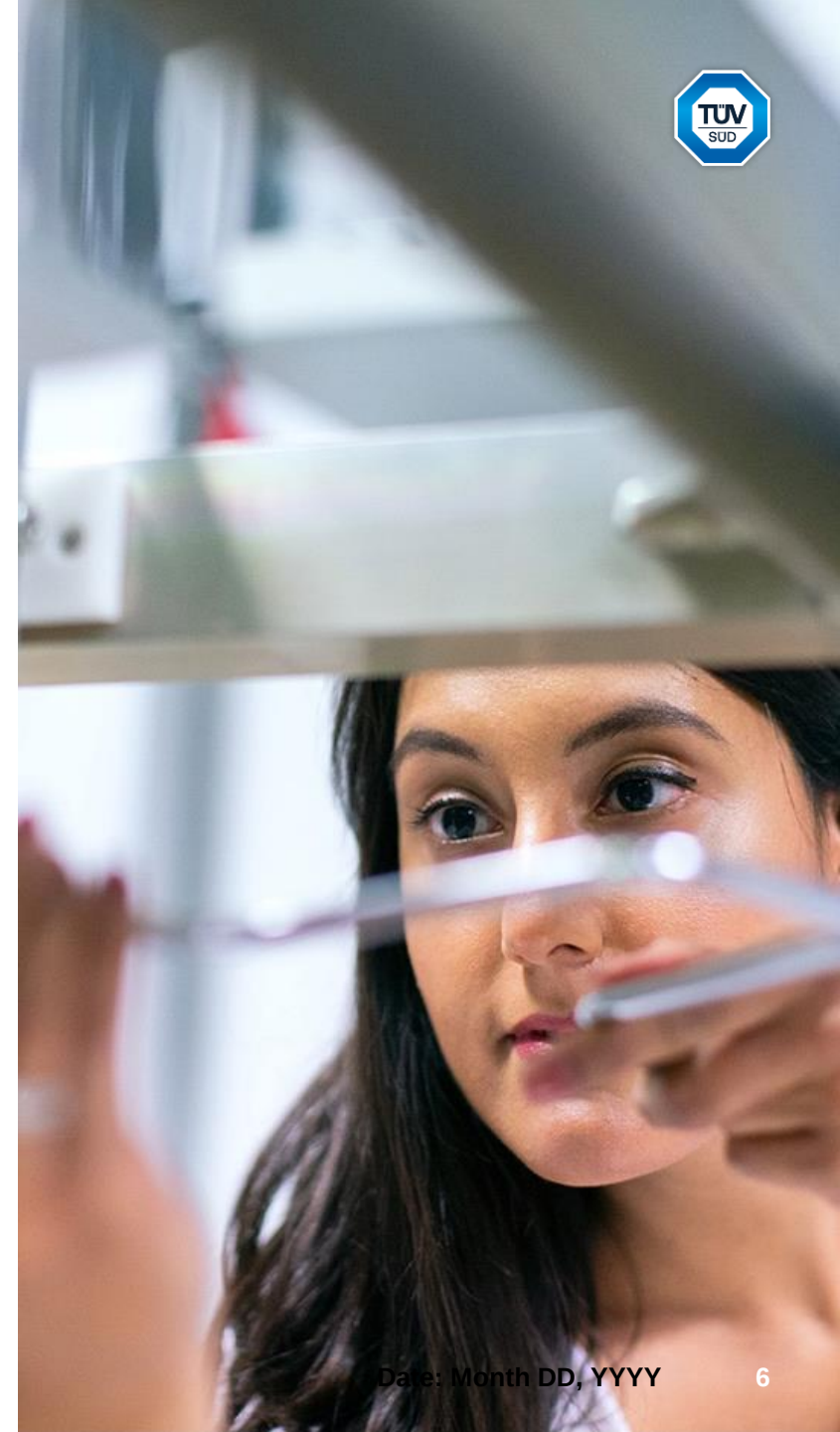


# Module 1

## INTRODUCTION

In this module

- Fail to Shutdown
- Case Study
- Risk Terminology
- Overview of PHA
- History of PHA
- Scenario 1



# Fail to Shutdown

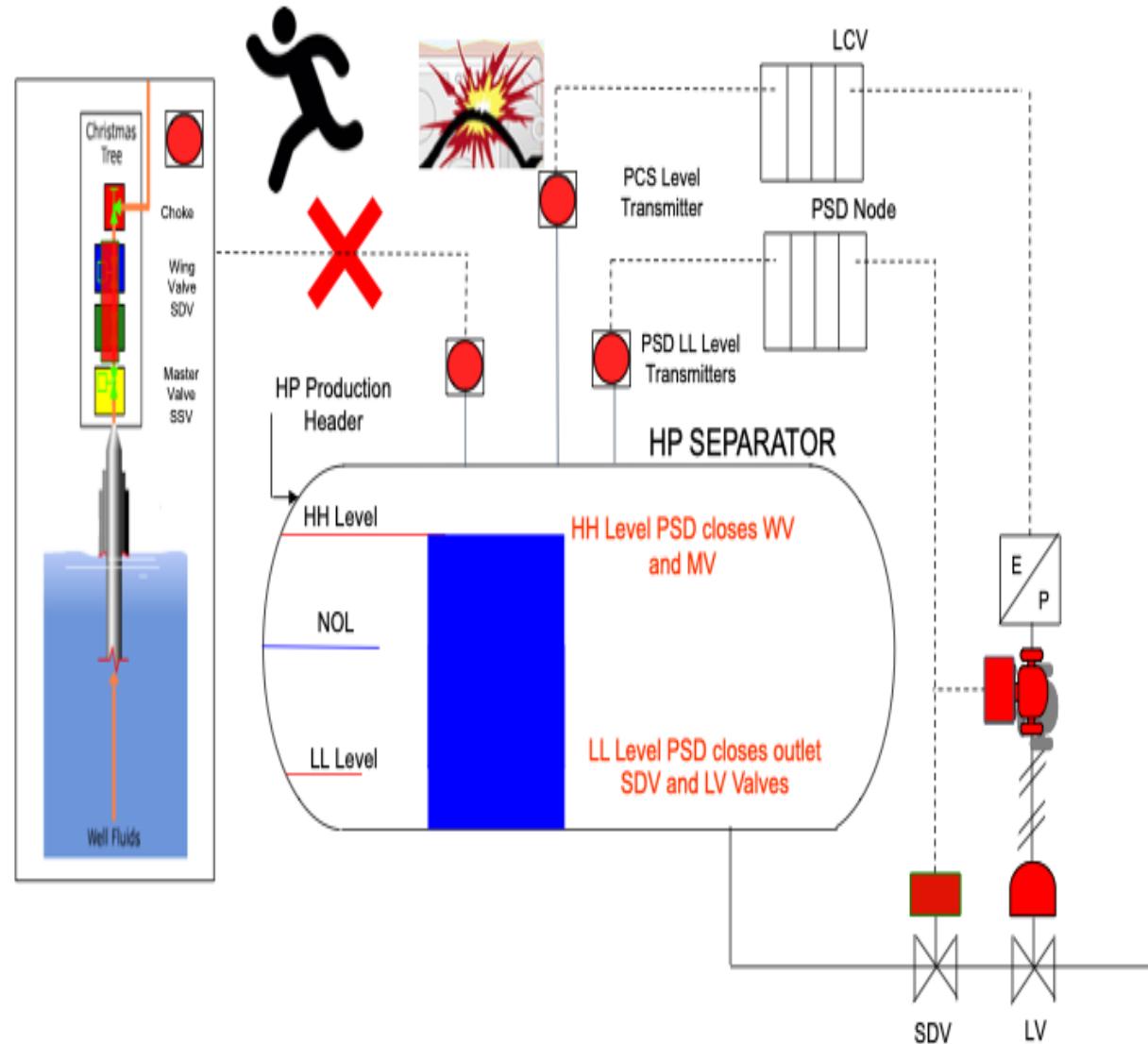
- level controller on HP Separator instantaneously went from 50% to 100% due to voltage fluctuation from an earthing fault & In response to this, the level control valve on separator outlet went fully open.
- Within 1 minute, the level in HP separator A dropped causing low alarm on PSD level transmitter. The level kept dropping and the oil outlet Shut down Valve was closed on Low Low limit. The level in HP separator A rapidly increased toward High High limits.



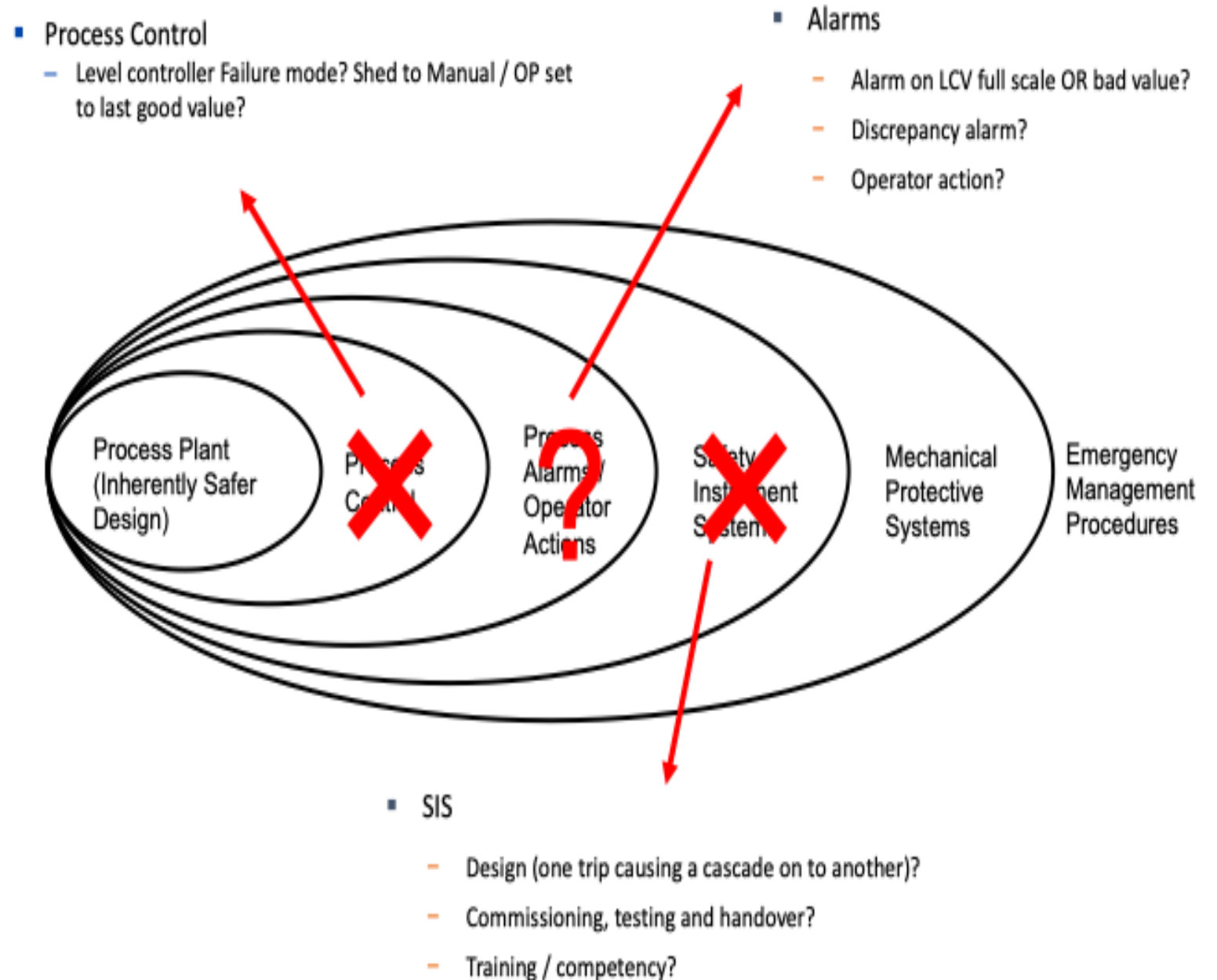


# Summary of Events

In your opinion ... What are the possible reasons that lead to this sequence of events and in the future How can we prevent this from happening again?



# Questions to be answered ?

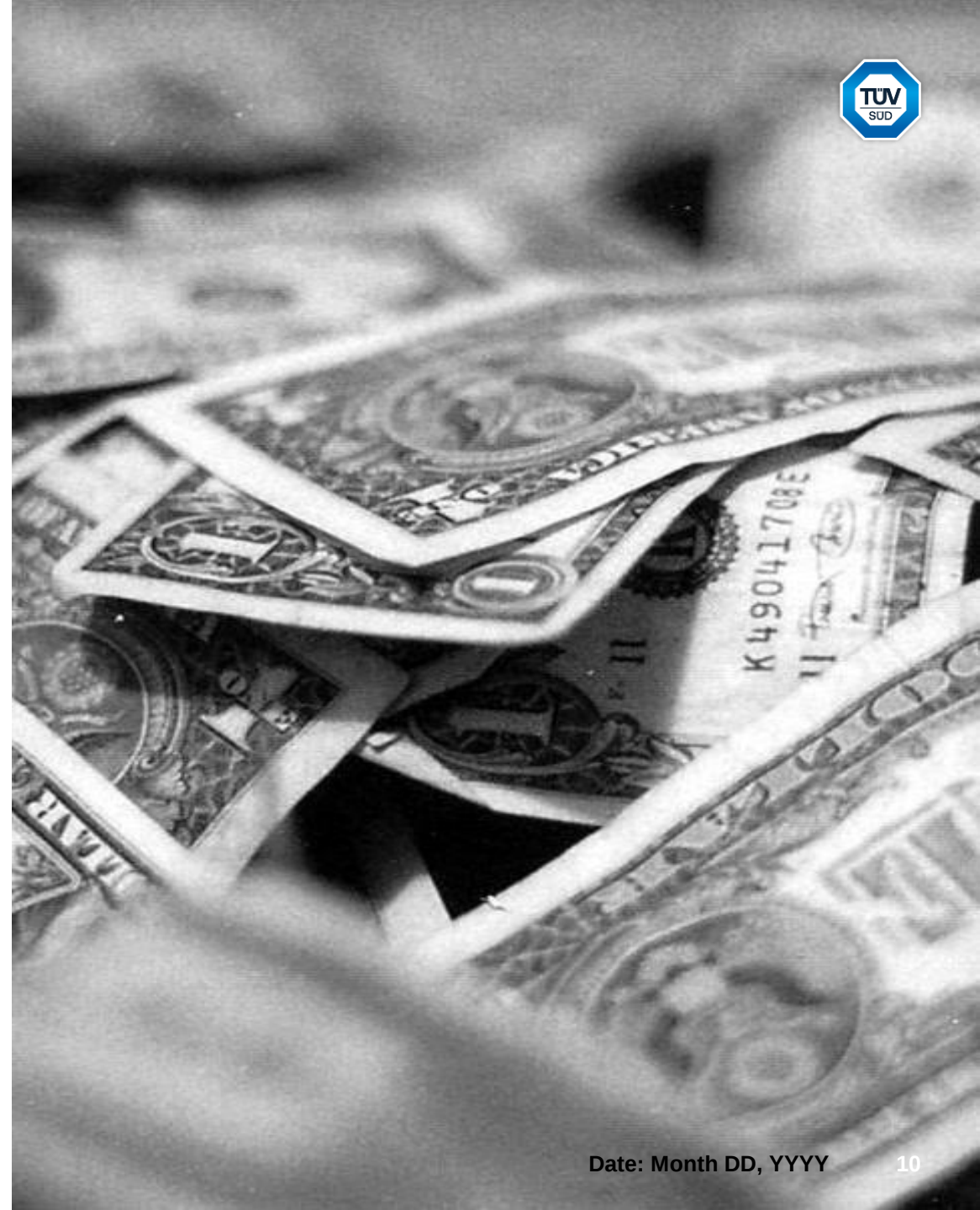




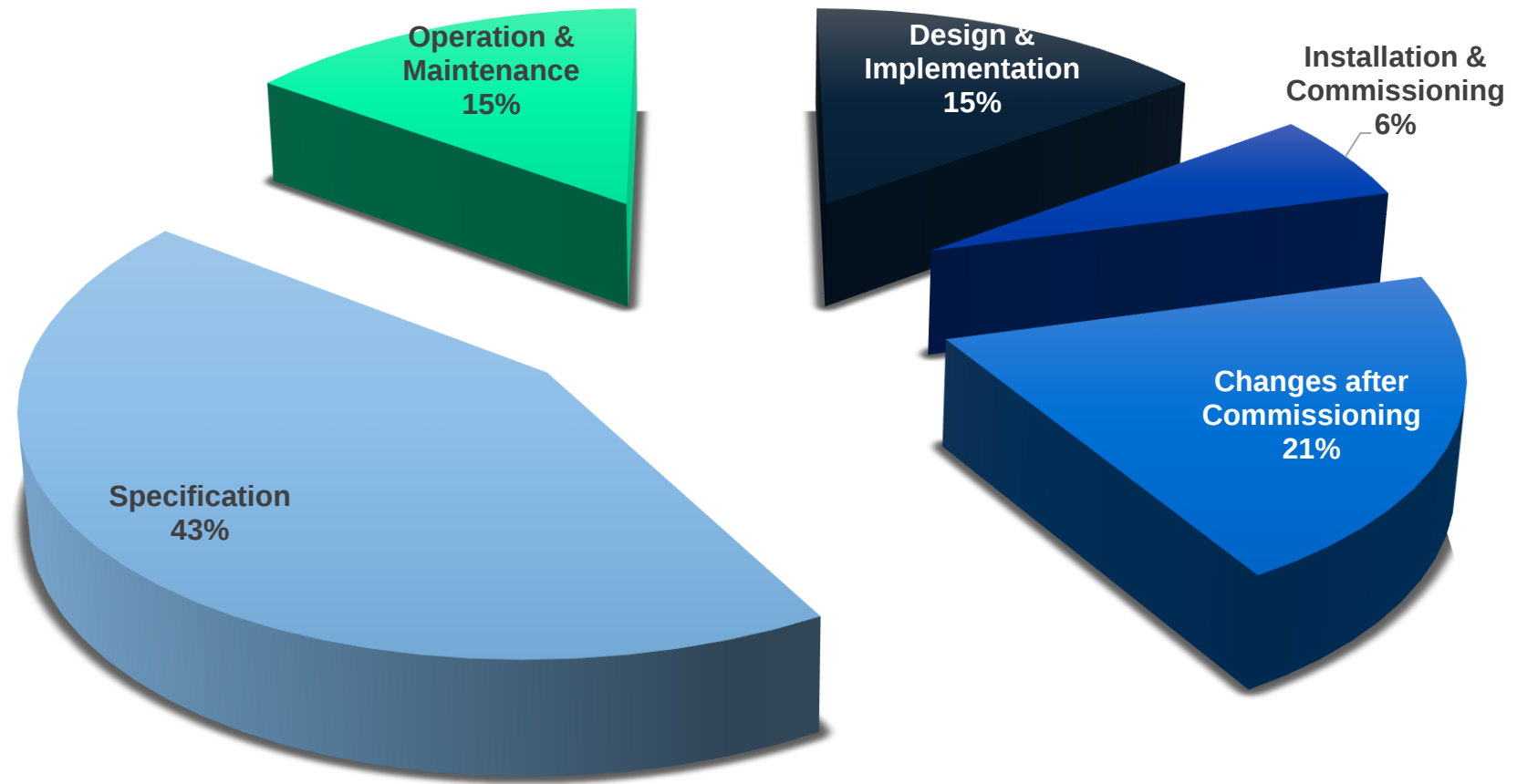
# Is safety expensive?



- Why should we invest in safety?
  - You think safety is expensive, try an accident.
  - Today an accident costs as a minimum 10x as much as it cost to build the plant
  - 2M people a year die from industrial accidents
  - We have had terrible accidents in the past
  - We learnt, but accidents with serious impact still happen today
- Training is one way to help people become more aware and knowledgeable about safety



# HSE Study of Accident Causes



■ Design & Implementation   ■ Installation & Commissioning   ■ Changes after Commissioning  
■ Specification   ■ Operation & Maintenance



# Hazardous Event

The release of a material or energy that has the potential for causing harmful effects to:

- The plant personnel
- The surrounding community at large
- The environment





# What is Risk?

Risk relates two important factors:

How much of what causes how much damage to whom (or whatever else) from the hazardous event, i.e., the Consequence.

How often the hazardous event can be expected to occur, i.e., the Frequency or Likelihood.

$$\text{RISK} = \text{CONSEQUENCE} \times \text{FREQUENCY}$$



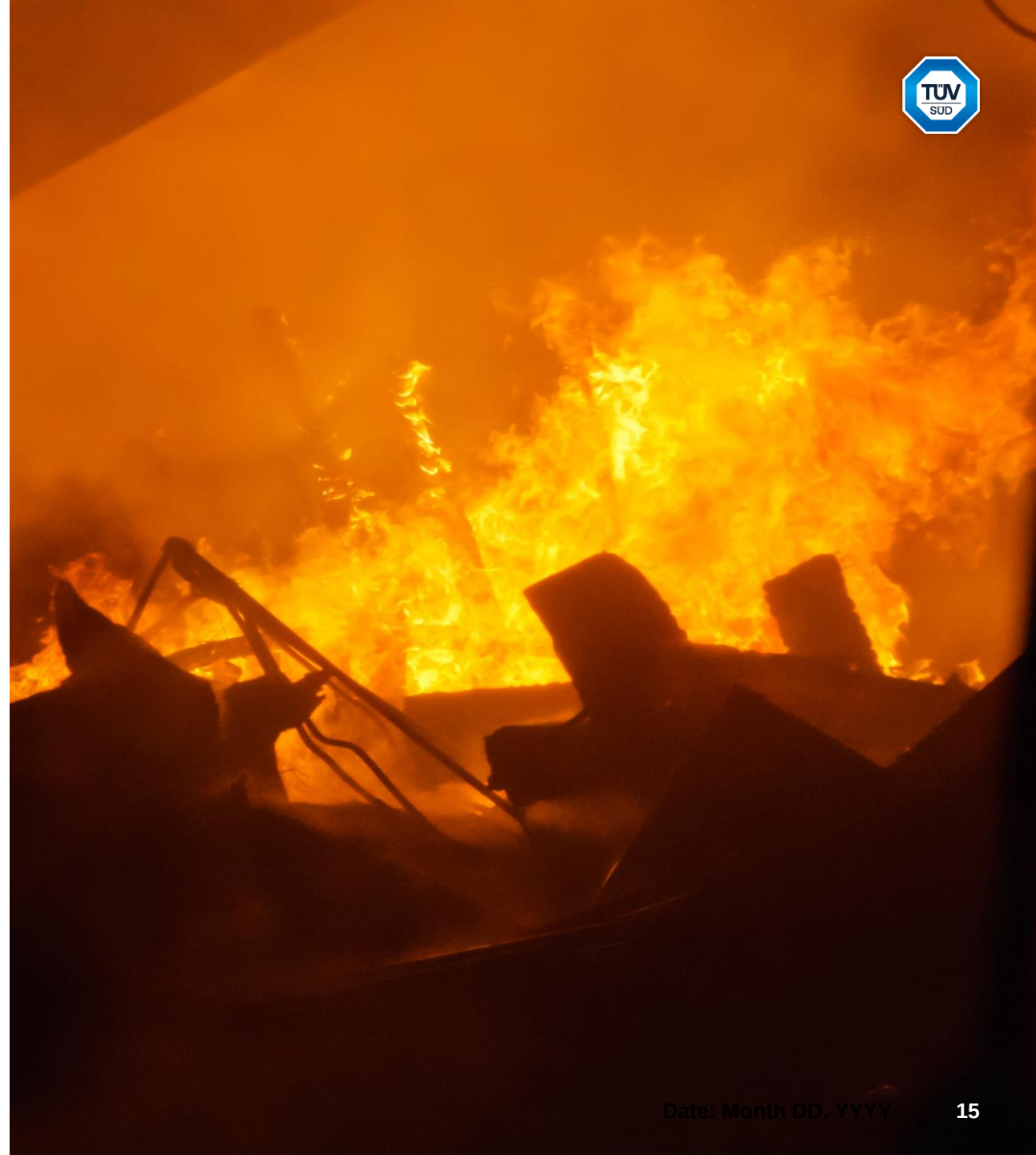
# Hazard Identification

Hazard Identification is fundamental to the safe design and operation of any system, be it a process plant or any other facility. The tools used vary according to the situation but they are all rigorous, systematic and depend to a greater or lesser extent on the knowledge of team members that will usually contain some form of expertise



# Typical incidents to be Concerned

- Toxic gas clouds;
- Asphyxiates;
- Fires (jet fires, pool fires, fireballs);
- Explosions ;
- Hazardous liquid spills;
- Combustible dusts;and
- Corrosive substances.





# Risk Terminology

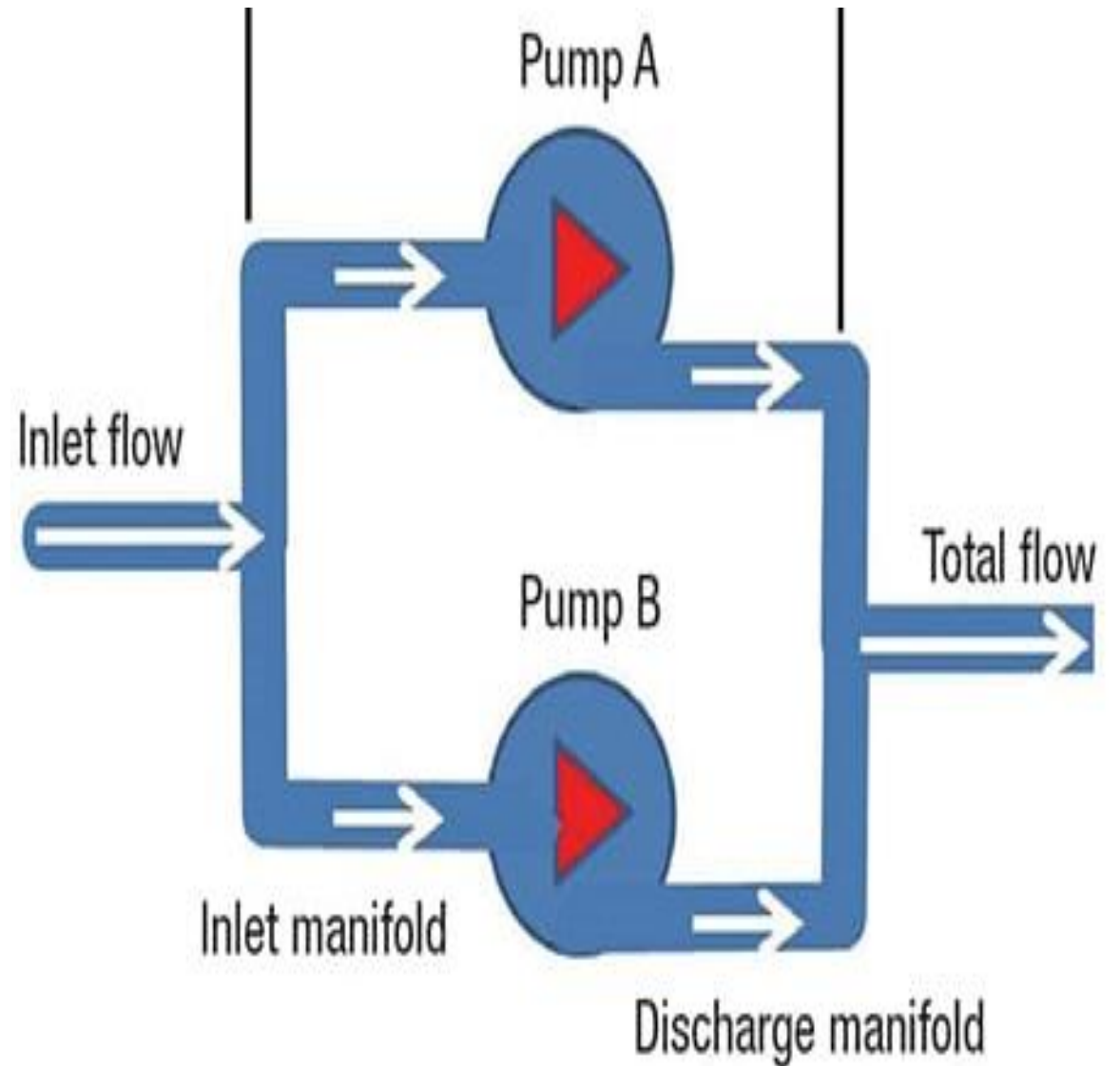
- BLEVE
- Combustible
- Explosion
- Fireball
- Flammable
- Flash Point
- Lower Explosive Limit (LEL)
- Upper Explosive Limit (UEL)
- Vapor Cloud Explosion (VCE)
- Process Safety time



# Double (or Multiple) Jeopardy

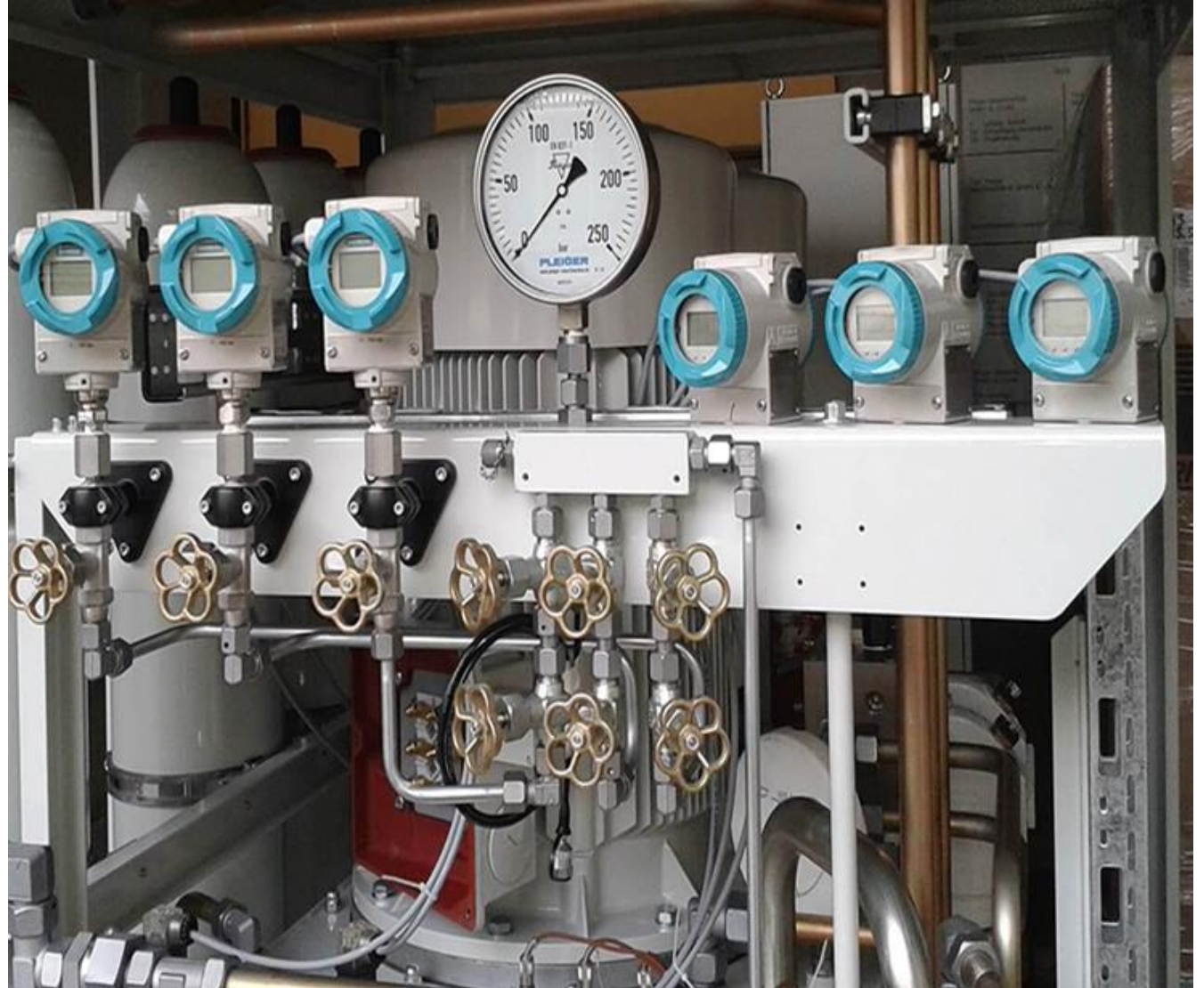


The chance that two (or more) unrelated events or incidents will occur at the same time. (It is important to note that two (or more) events or incidents arising from a common cause do not qualify).



# Confusion in Terminology

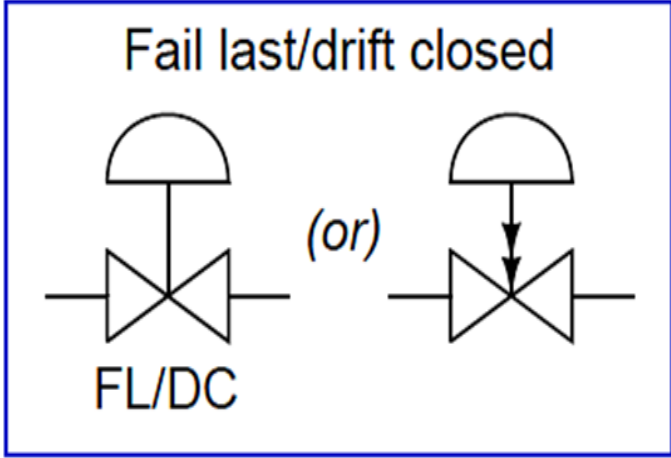
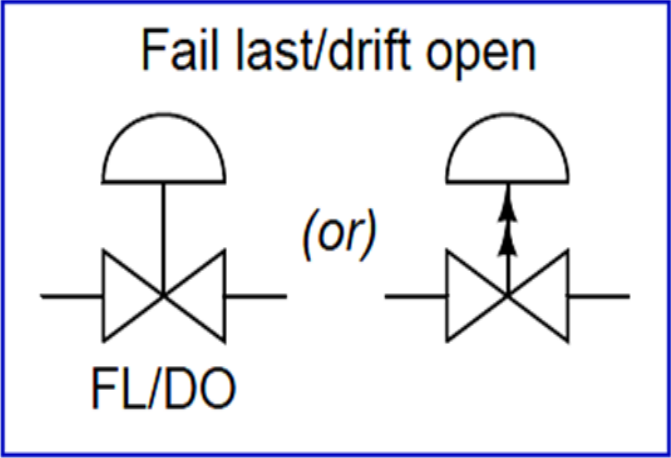
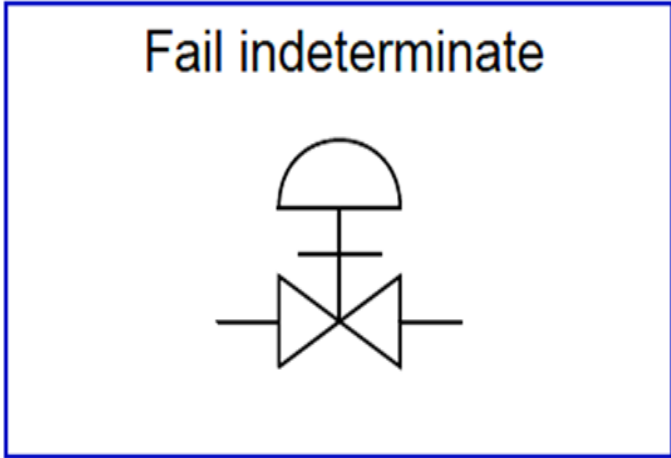
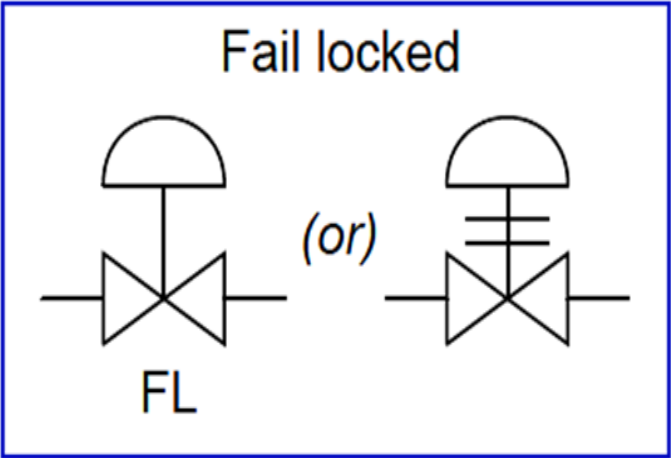
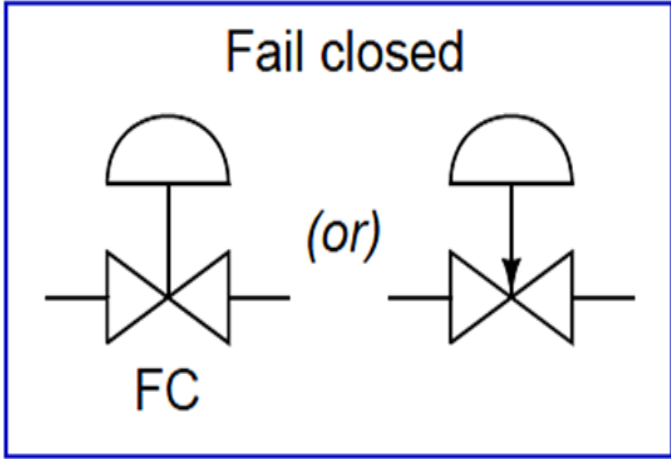
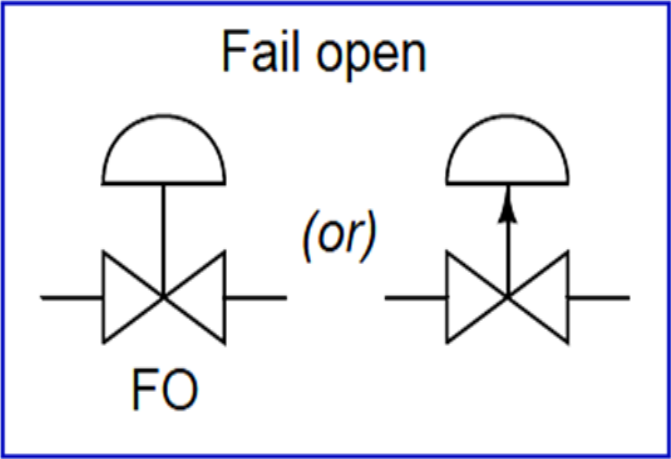
- DOUBLE-JEOPARDY
- SIMULTANEOUS FAILURES
- COMMON CAUSE





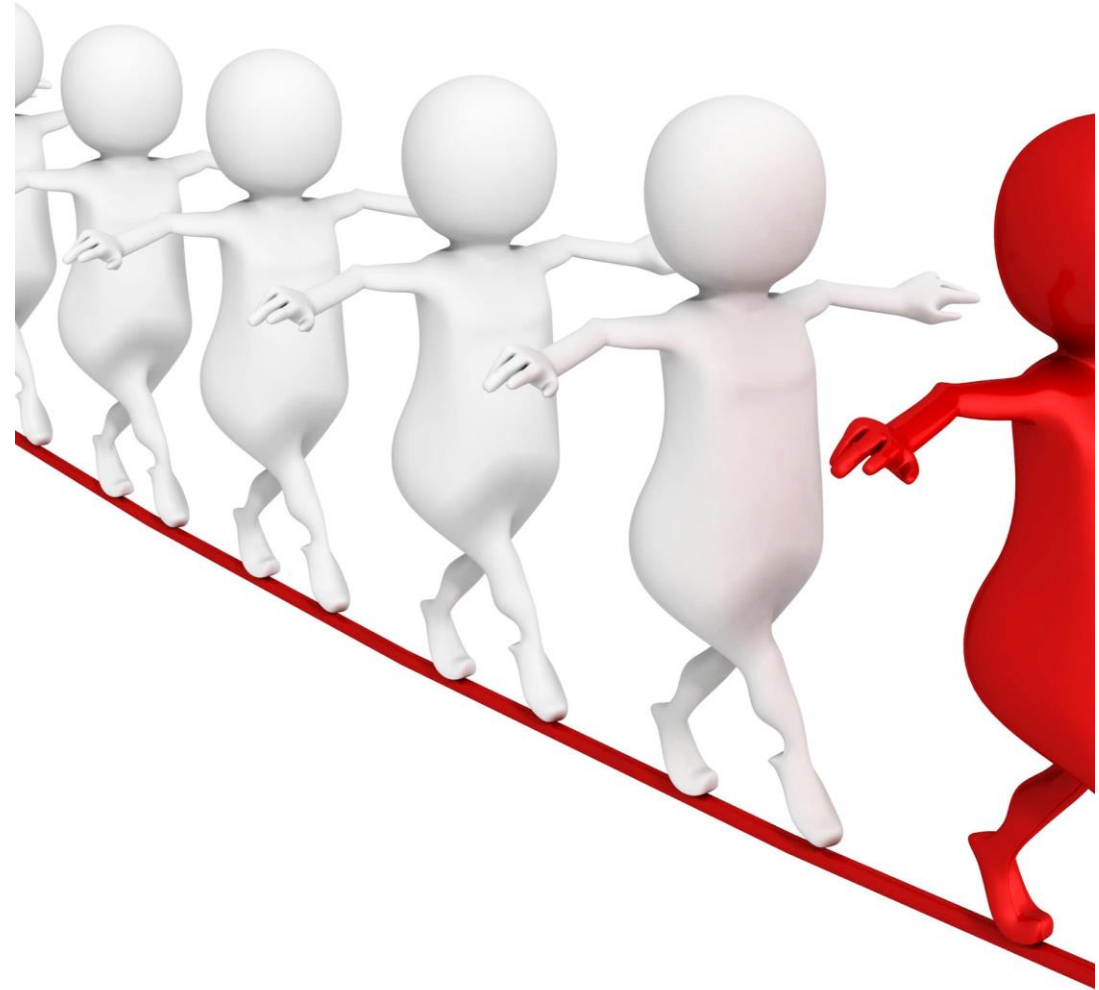
# Fail Safe

Design features which provide for the maintenance of safe operating conditions in the event of a malfunction of control devices or an interruption of an energy source (e-g., direction of failure of a pneumatically actuated valve on loss of instrument air). Features incorporated for automatically counteracting the effect of an anticipated possible source of failure. A system is fail-safe if failure of a component, signal or utility initiates action that return the system to a safe condition.



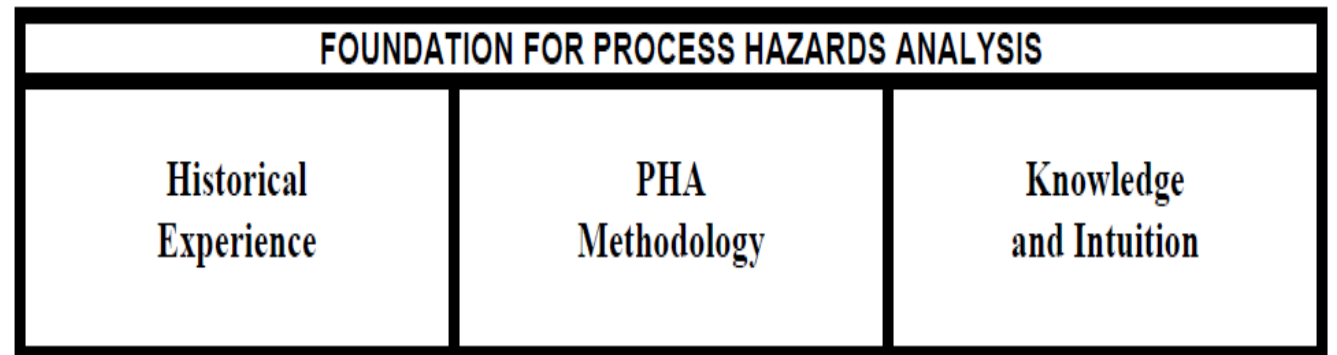
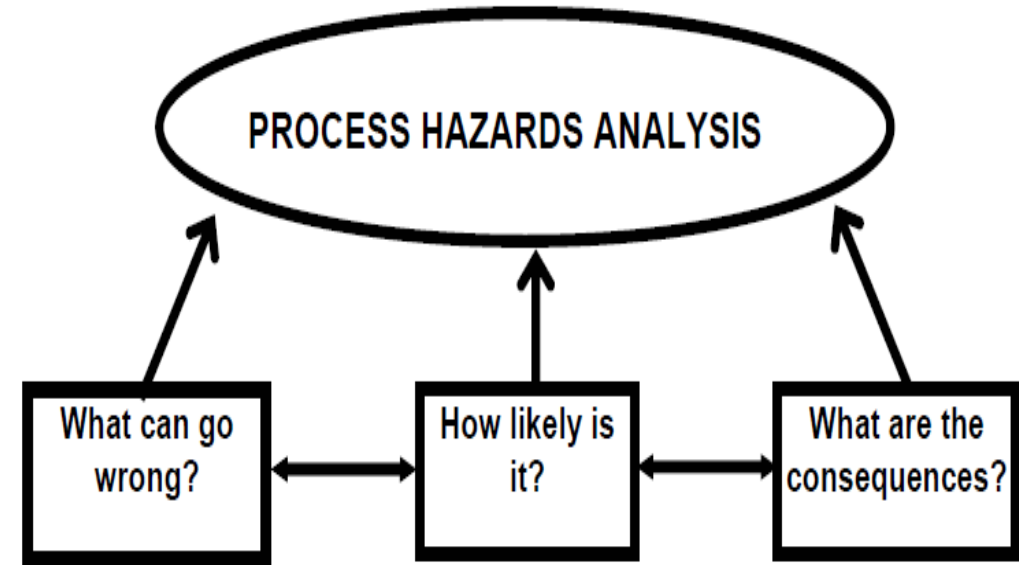
# Overview of PHA

- A PHA is a systematic multidisciplinary team study. It focuses on identifying and analysing the significance of potential process hazards and on making initial recommendations for eliminating and/or reducing the consequences of potential incident/accidents.
- A PHA is the foundation of any Process Safety Management Program.
- A PHA is interested in the potential causes, likelihood and consequences of process incidents.
- A PHA works by combining the experience, knowledge and intuitive imaginations of expert team members with a selected analytical methodology.
- A PHA provides companies with the information necessary to make operating decisions, to help improve safety, and to manage the risk of operations.
- Various hazard identification methodologies provide flexibility according to time scope and objectives of study.
- A PHA should be conducted several times during a facility's design, construction and operating life cycle.



# Overview of PHA

- Some methodologies not only identify hazards, but also operability problems.
- A PHA assigns qualitative likelihood and severity ratings from which a relative risk ranking can be estimated.
- A PHA identifies high level hazards for possible further quantitative risk analysis.





# History of PHA

- HAZOP, the first formal PHA, was developed in the UK at ICI over 30 years ago. Other methodologies have followed as requirements for less comprehensive and time consuming reviews have emerged.
- The occurrence of major industrial accidents and the subsequent forceful safety and environmental legislation throughout the world has led to Process Safety Management (PSM) or Process Hazards Management becoming an industry standard.
- Companies have become increasingly aware that operating a safer facility leads to a more profitable business and that, in the long run, safety is in the best financial interest.
- Development of software to aid in the sometimes tedious task of PHA has led to its adoption throughout the process chemical industry.
- PHA was legislated (1992) in the USA as part of OSHA CFR 29, Part 1910.
- PHA is part of American Petroleum Institute (API) Recommended Practice 750, 1990, which stands as the recommended standard for Canadian process industries.
- OSHA 29 CFR, British Standards 8800 and Norwegian regulations have become the world standards.



# Scenario 1

Recently, the K-I polymerization unit at OilChem Corporation exploded, killing three workers. An investigation showed that a pressure control system on a feed line to the reactor, which was designed to keep the feed under pressure and in a liquid state, failed, allowing the feed to vaporize. The vaporized feed continued to flow into the reactor. The flow control meter on the feed line did not register the vaporized feed as a flow, causing the operator to believe that a high-level alarm on the reactor was false. As a result, the operator by-passed the safety interlock on the feed line, causing the vessel to over-pressurize and explode.





# Exercise

## Case Study

On the 6th July, 1988, safety lapses aboard the Piper Alpha oil rig resulted in a series of devastating explosions. This and related process safety accidents are well-known among chemical engineers. Situated 140 miles off the coast of Aberdeen, Scotland, the Piper Alpha oil rig disintegrated in under 3 h, claiming the lives of 165 of the 226 men on board, plus those of 2 rescue crewmen. With only 61 survivors of the accident and approximately \$3.4 billion total insured damages, the Piper Alpha disaster remains one of the worst such events in the Oil & Gas sector

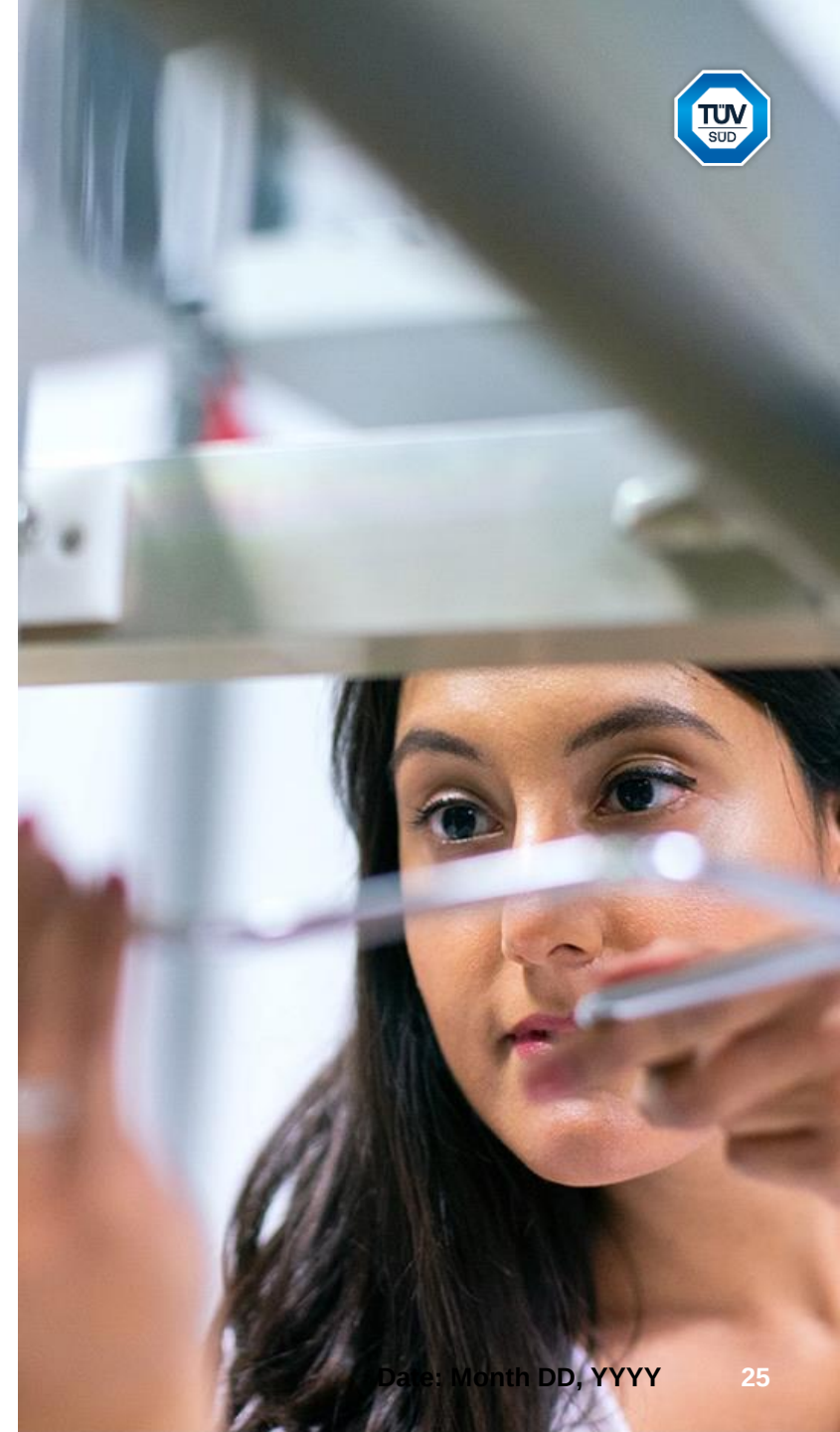




# Summary

What we have learned in the module

- HSE Study of Accident Causes
- Hazardous Event
- What is Risk?
- Typical incidents that Concern Us
- Risk Terminology
- History of PHA



# Exercise 1 - Questions



Q1).....The release of a material or energy that has the potential for causing harmful effects .

- A. Risk
- B. Hazard Events
- C. Consequence
- D. Accident

# Exercise 1 - Questions



Q2) During Hazard Identification, Systematic techniques is not recommended as it will affect on group creativity .

- A. True
- B. False
- C. Sometimes Depend on the process scope itself



# Exercise 1 - Questions



Q3) As per HSE Studies the causes for accident is .....

- A. Specifications
- B. Maintenance
- C. Commissioning
- D. Changes after Installations
- E. All of the above

# Exercise 1 - Questions



Q4) .....the first formal PHA, was developed in the UK at ICI over 30 years ago. Other methodologies have followed as requirements for less comprehensive and time consuming reviews have emerged.

- A. What If
- B. LOPA
- C. HAZOP
- D. FMEA

# Exercise 1 - Questions



Q5) A PHA assigns qualitative likelihood and severity ratings from which a relative risk ranking can be estimated.

A. True

B. False

Q6) A PHA should be conducted One time only during a facility's design ,before the start-up and introducing the hydrocarbon to the plant .

A. True

B. False



# Exercise 1 - Questions



Q7) The chance that two (or more) unrelated events or incidents will occur at the same time. (It is important to note that two (or more) events or incidents arising from a common cause do not qualify).

- A. Fail Safe
- B. Consequence Failure
- C. Dangerous Failure
- D. Double Jeopardy

# Note



# Any Question?



**Follow us on:**



[tuvsud.com](https://tuvsud.com)  
[info@tuvsud.com](mailto:info@tuvsud.com)



# CERTIFIED PHA - HAZOP LEADER

## PROCESS SAFETY MANAGEMENT



01

**Module 1**  
INTRODUCTION

02

**Module 2**  
PROCESS SAFETY MANAGEMENT

03

**Module 3**  
HAZOP

04

**Module 4**  
REHAZOP & LOPA

05

**Module 5**  
Checklists

06

**Module 6**  
WHAT IF & FMEA

07

**Module 7**  
LEADERSHIP

08

**Module 8**  
BOWTIE ANALYSIS

The background image shows a worker in a yellow hard hat and a blue and red safety vest, looking towards a large industrial facility. The facility has several tall smokestacks and complex piping. The scene is set in a field of tall grass under a dramatic, cloudy sky at sunset or sunrise. The title '2 PROCESS SAFETY MANAGEMENT' is overlaid in large, bold, red letters on the left side of the image.

# 2 PROCESS SAFETY MANAGEMENT

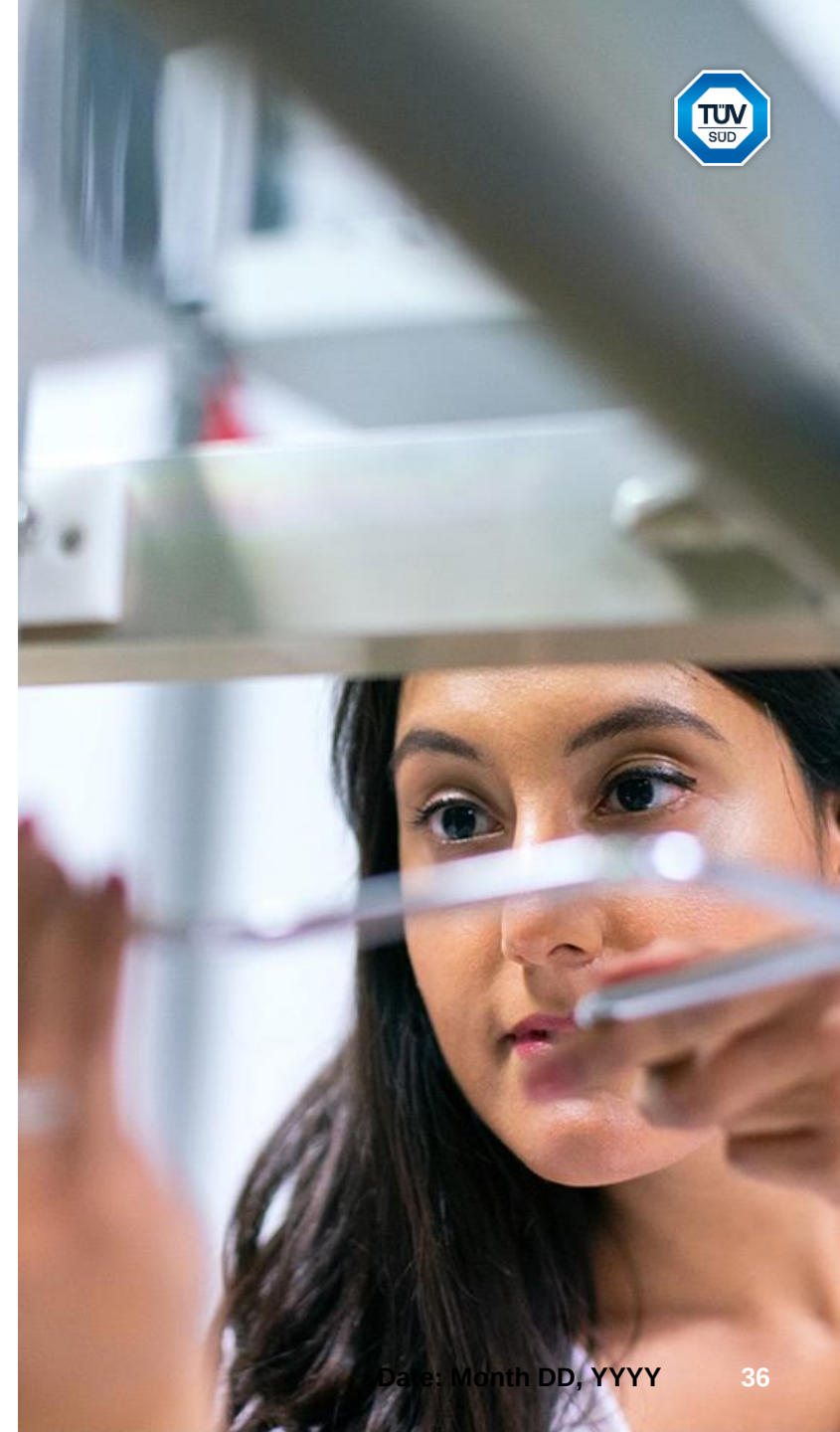


# Module 2

## PROCESS SAFETY MANAGEMENT

In this module

- Process Hazard Analysis
- Risk-Based Decision Process
- Quantitative & Qualitative HAZARD Analysis
- Elements of Facility Risk
- Process Risk Reduction Strategies
- Human Factors in Facility Risk
- PHA Teams
- General PHA Procedure Flow Chart
- Scenario 2



# Process Hazard Analysis

- Process hazard analysis is about applying the basic principles of probability and risk management to make long term value added decisions.
- The starting point for any good decisions coming for a process hazard analysis should be a shared understanding of what a process hazard analysis actually trying to achieve. When designing a complex process to operation safely yet productively, we need a process that everyone understands: one that facilitates discussion and decision.





# Risk-Based Decision Process



- Risk has two elements. Probability and Severity. Risk-based decision is choosing the best of a number of alternatives to maximize the resources available and minimize the risks. The value to risk-based decisions occurs not when you have complete control and knowledge of the future prospects but when you don't.
- 1) Group can lose focus and needs to be re-focused**
    - Discussion can go off on tangents. Your team can lose focus and people can start losing confidence in the decision making process. A good facilitator knows when to focus the discussion to the problem at hand.
  - 2) Opinions diverge then converge**
    - At the start of each scenario individual members of a group should contribute their own points of view. Not everyone will agree on a severity of a consequence or the likelihood of an event. This is because everyone has different experience and backgrounds.

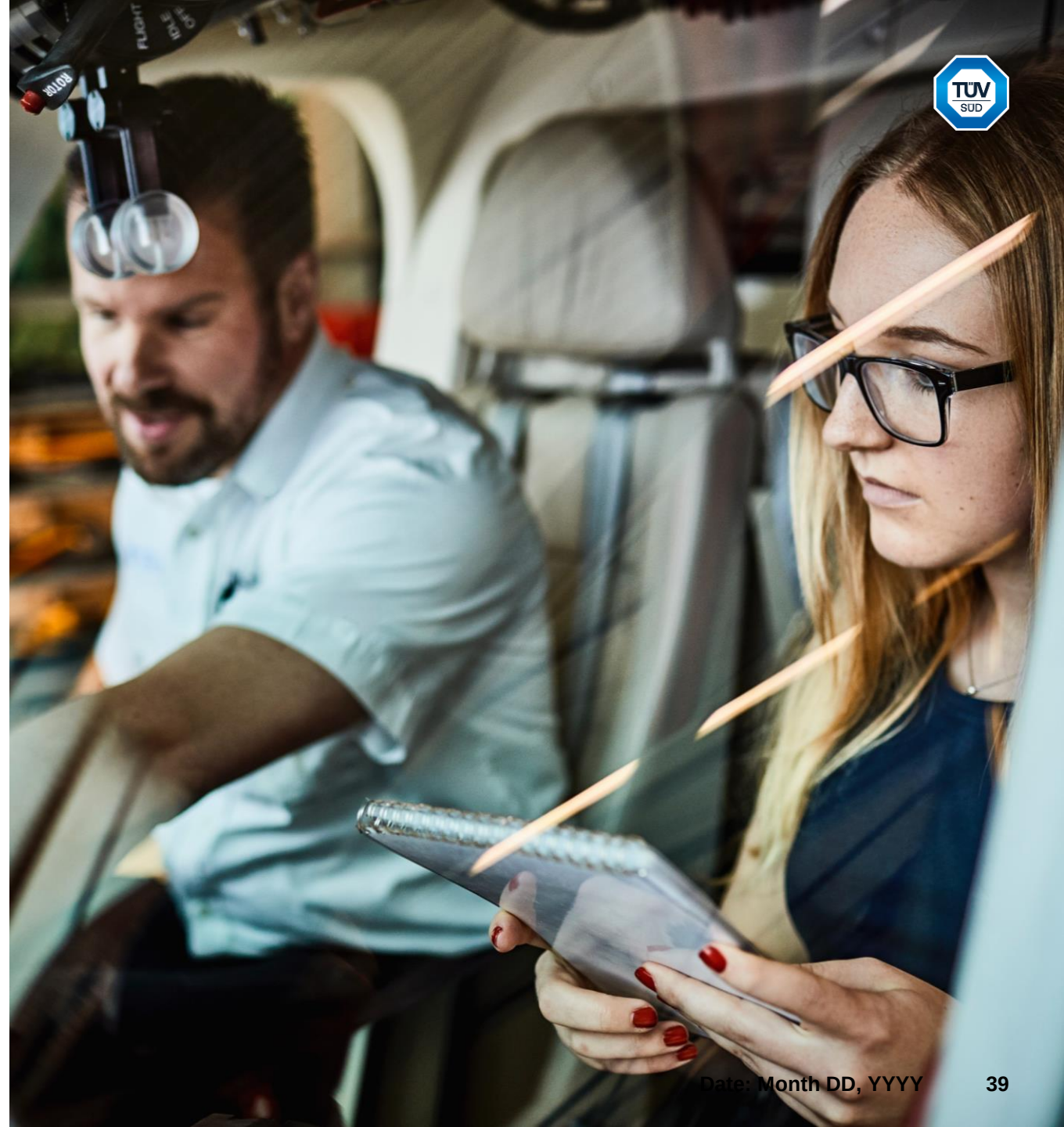


# Quantitative and Qualitative Hazard Analysis

- PHA is the initial predictive identification of potential hazards.
- Risk Analysis provides a statistically based quantitative assessment of the probability and consequence of major hazards identified in a PHA.
- Both qualitative and quantitative hazard analyses are important in identifying and analysing risk.

## PHA

- Initial predictive identification of all potential hazards - estimates likelihood and severity, suggests improvements
- Use on Every Project - at every stage from concept through decommissioning
- Qualitative - based on the experience, knowledge and creative thinking of workers involved in the process
- Multidisciplinary Team

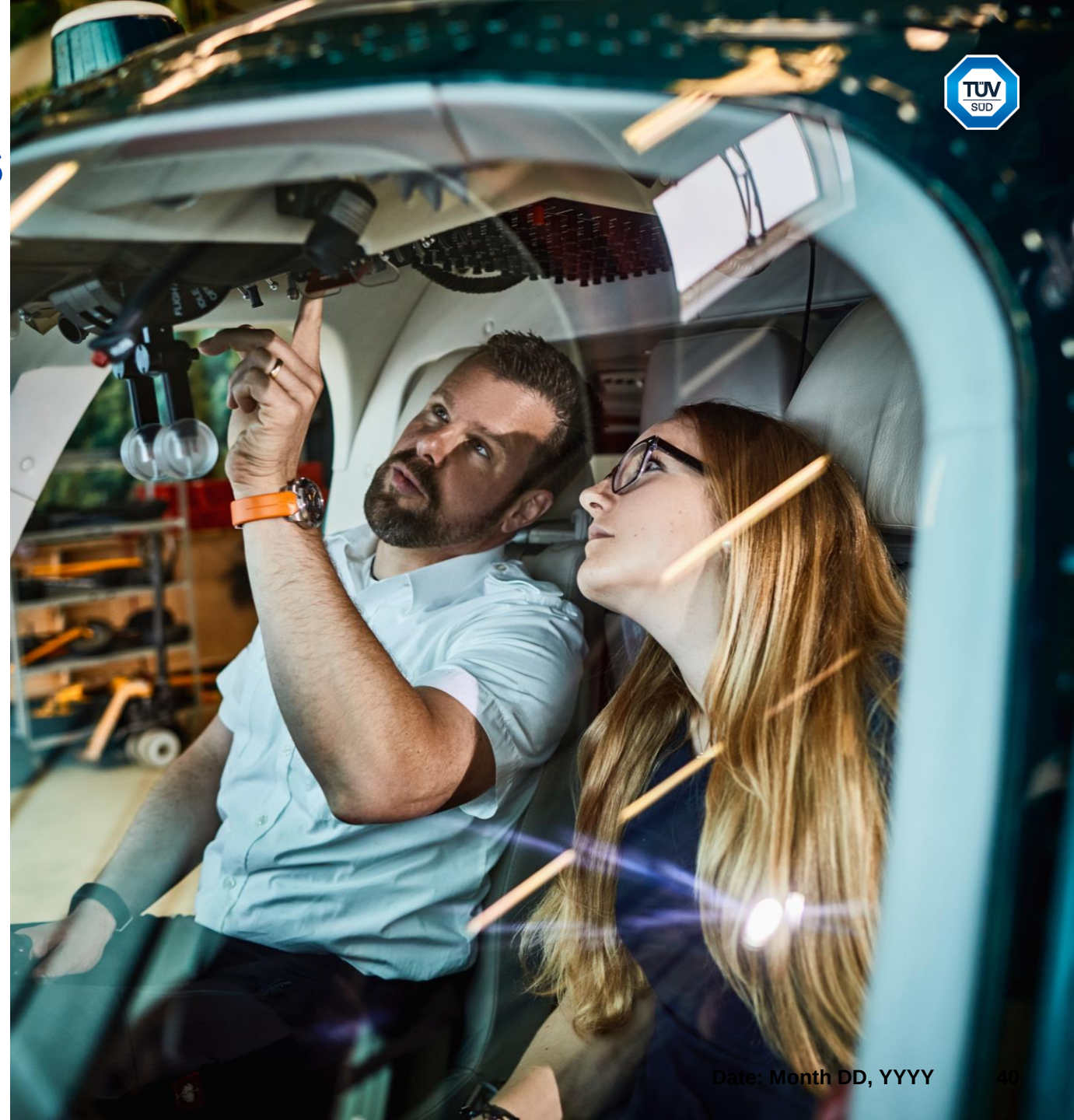




# Quantitative and Qualitative Hazard Analysis

## RISK ANALYSIS

- Subsequent assessment of major hazards only – statistically based probability / consequence hazard assessment.
- SELECTIVE - if the potential exists for a catastrophic accident or if no easy and obvious solution to identified hazard is evident.
- QUANTITATIVE - requires extensive statistical data and specialized expertise – very costly.
- One or Two Specially Trained People.





# Hazards Identification and Assessment

- identifies a wide range of hazards .
- identifies actual and hidden potential hazards
- allows hazards to be prioritized
- identifies high risk hazards
- provide recommendations for mitigating consequences
- highlights opportunities for improving operability





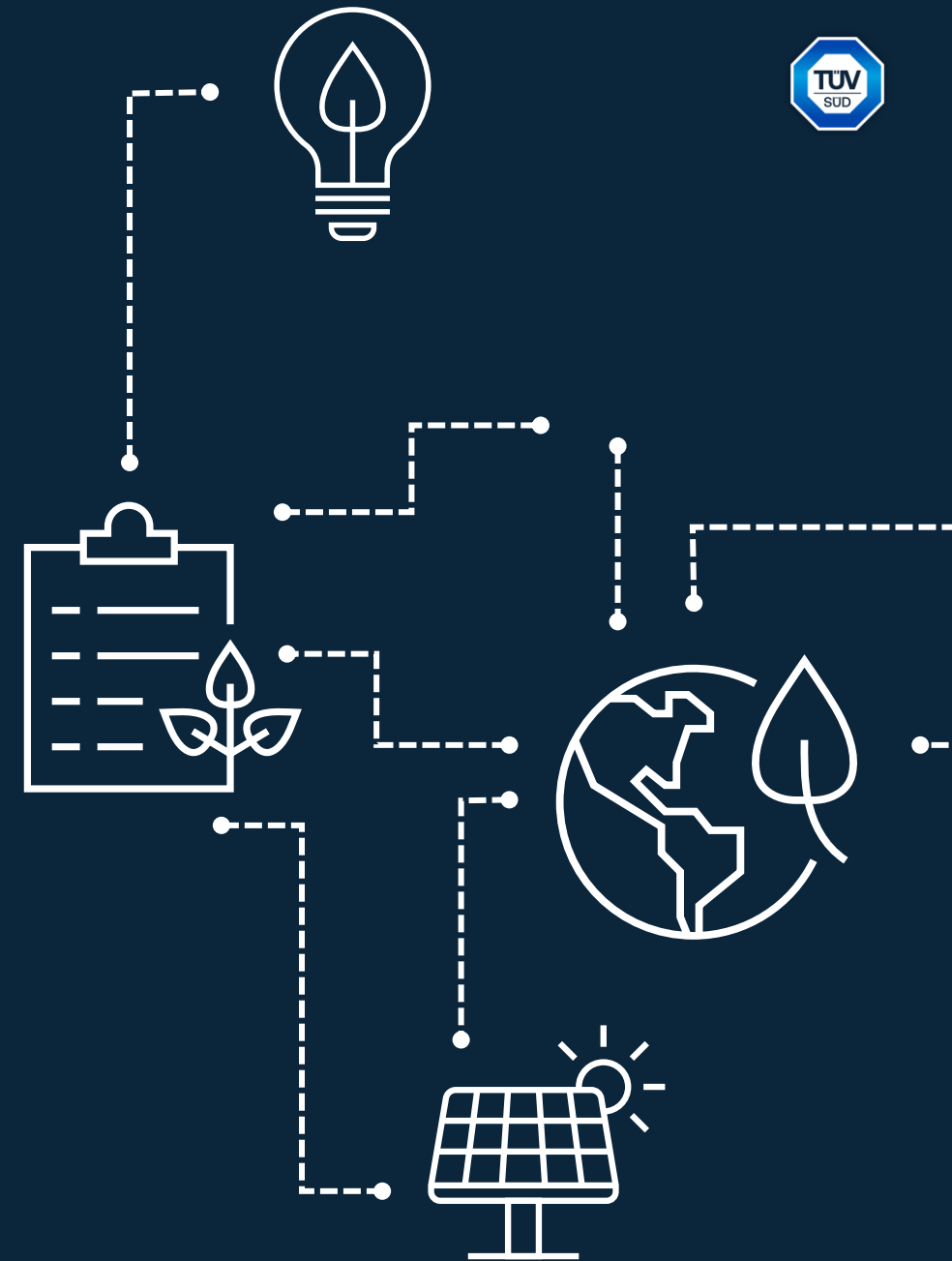
# Hazard Controls

- design layout information can identify design errors and highlight opportunities for debottlenecking and improving operability.
- identifies a need for formal operating, maintenance and emergency procedures
- highlights weaknesses in existing procedures
- can be adapted to perform Job Hazard Assessments and Critical Task Analyses
- identifies the need for a refresher training schedule



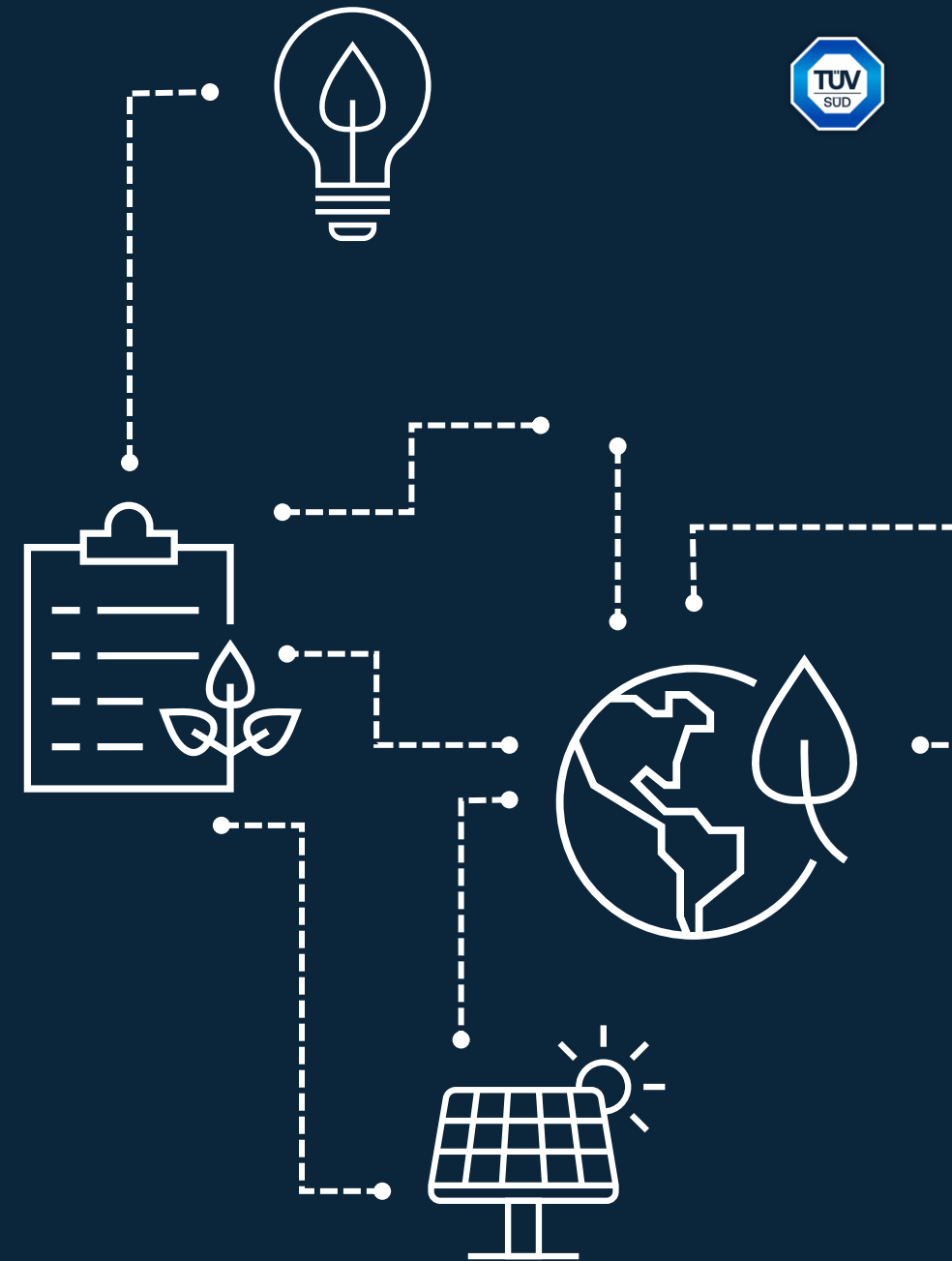
# Hazardous Materials

- identifies potential immediate and long term health concerns
- identifies potential chemical interaction hazards
- identifies gaps in existing precautionary procedures
- can provide recommendations for mitigating consequences of accidents



# Elements of Facility Risk

- **Initiating events** are the first events in an accident sequence, the event or action that sets off a chain reaction.
- **Propagating events** are the secondary events that link an initiating event to an accident outcome.





# Process Risk Reduction Strategies

- Operator Control Systems (Alarm , DCS, ESD , F&G)
- Mitigation Systems (PSV, Bund, Dike , Flare)
- Procedure
- Emergency Plans
- Training Systems
- Management
- Design



# Human Factors in Facility Risk



- Human error is seen as the incompatibility of task demands and human emotional, mental and physical capabilities. Human error has been the major cause of almost all catastrophic accidents in the chemical process industry .
- The PHA objective, in considering human factors in facility risk.
- Human error is either an active or a latent (waiting to happen) error.
- **Active Human Error**
- Active human error has an immediate and direct effect on the cause of a hazardous situation or is the direct initiator of a chain of events, which leads to an accident.
- **Latent Human Error**
- Latent human error is different in that the consequences of the error may only become dynamic after a period of time when the condition caused by the original error combines with other errors or system failures to bring about unsafe conditions.





# PHA Teams





# PHA Teams

- A PHA is performed by a multidisciplinary team experienced in engineering, operations and maintenance. Other relevant experts should be included as required. At least one member of the team should have knowledge specific to the process being evaluated and at least one member should be knowledgeable in the PHA methodology being used and impartial in the evaluation.
- As few as two or three and as many as seven or eight depending on the methodology chosen and the size and complexity of the facility. Too many participants reduce the efficiency of any PHA.



# Advantages of team approach



- Range of expertise and experience creates a wide information pool base for decision-making.
- Representatives from different “cultural groups” in a facility can bring multiple perspectives to problems and the implications of proposed actions.
- Groups can make higher quality decisions because they have a greater combined capacity to comprehend a problem’s complexities and its alternative solutions.

# Disadvantages of team approach



- Time Pressure
  - Social Pressure
  - Ego Pressures
- 
- It is the responsibility of both participants in PHAs and the leaders of PHA teams to recognize the negative potential within the group and work towards creating group cohesion and efficiency.



# Responsibility of Group Participants in PHAs

- Be on time - commit to schedule and study goals.
- Remain focused.
- Respect the ideas of others.
- Actively participate.
- Critically evaluate ideas not the person
- Contribute all relevant information and ideas.
- Be prepared for some degree of conflict.
- Think in the long term as well as the here and now.
- Be prepared to find out if you do not know.



# Thinking Modes

- objective thinking “just the facts” (interested in concrete details)
- intuitive thinking (listen to your gut feeling)
- worst case thinking (What is the worst thing that could happen?)
- best possible scenario of what is practical and beneficial
- forward thinking of alternatives, solutions and linking of old and new
- “Big picture“ thinking that organizes and controls the detailed thinking process
- It is assumed and inferred by the P&ID being studied that product will normally flow from point A to B safely and without interruption to operation. To test this assumption it is questioned:
  - Could there be no flow?
  - How could it occur?
  - What would be the consequences of no flow?
  - Would the consequences be hazardous ?
  - What are the solutions?





# General PHA Procedure Flow Chart

- Define Node or system
- Hazard Identification
- Possible Hazard Consequence
- Identify Existing safeguards
- Risk Ranking
- Recommendation





# Objectives of a Good PHA Study

- To identify hazards, not to necessarily provide solutions to hazards.
- To provide the greatest possible confidence that all of the potential hazards are identified .
- To provide a qualitative estimate of the likelihood and the severity of potential accidents.
- To qualitatively evaluate the consequences of failed engineering and administrative controls.
- To provide management with a concrete and easy to use basis for making risk management decisions.
- To identify ways in which operability might be improved.
- To provide information which can be useful in improving future designs.
- To provide objective documented evidence of a thorough well conducted study for audit and insurance purposes.



# PHA Study required Information



- Material Safety Data Sheets (MSDS)
- process flowsheets and material balance information
- overview of the process and a process description
- PFD
- ESD logic diagrams
- operating and maintenance procedures
- list of safety critical components
- Emergency Response Plans (ERPs)
- plot plans and equipment layouts
- (P&IDs), Cause and effect
- SLD and area classification drawings
- flare, vent and relief system design basis
- relief valve specification sheets
- building ventilation design basis
- flare and gas detection design basis
- equipment failure history logs and failure analysis



# How do we identify Hazards?

- Identify potential loss of containment situations.
- Identify causes that can result in loss of containment.
- Identify potential consequences of loss of containment.
- Identify potential safeguards that may:
  - Prevent loss of containment
  - Mitigate or reduce the consequences (such as fire, explosion, toxic release)

**Depending on Step 1 to 4, actions may be introduced to reduce the hazard**





# Widely Used Methodologies to Identify Hazards

- Preliminary Hazards Analysis (PrHA).
- Hazard and Operability Analysis (HAZOP)
- Failure Mode and Effects Analysis (FMEA)
- What If Analysis
- Checklist
- What If + Checklist





# PHA

- A systematic effort designed to identify and analyze hazards associated with the processing or handling of highly hazardous materials; and
- A method to provide information which will help workers and employers in making decisions that will improve safety.
- **Process Experience Is a Must**





# Scenario 2



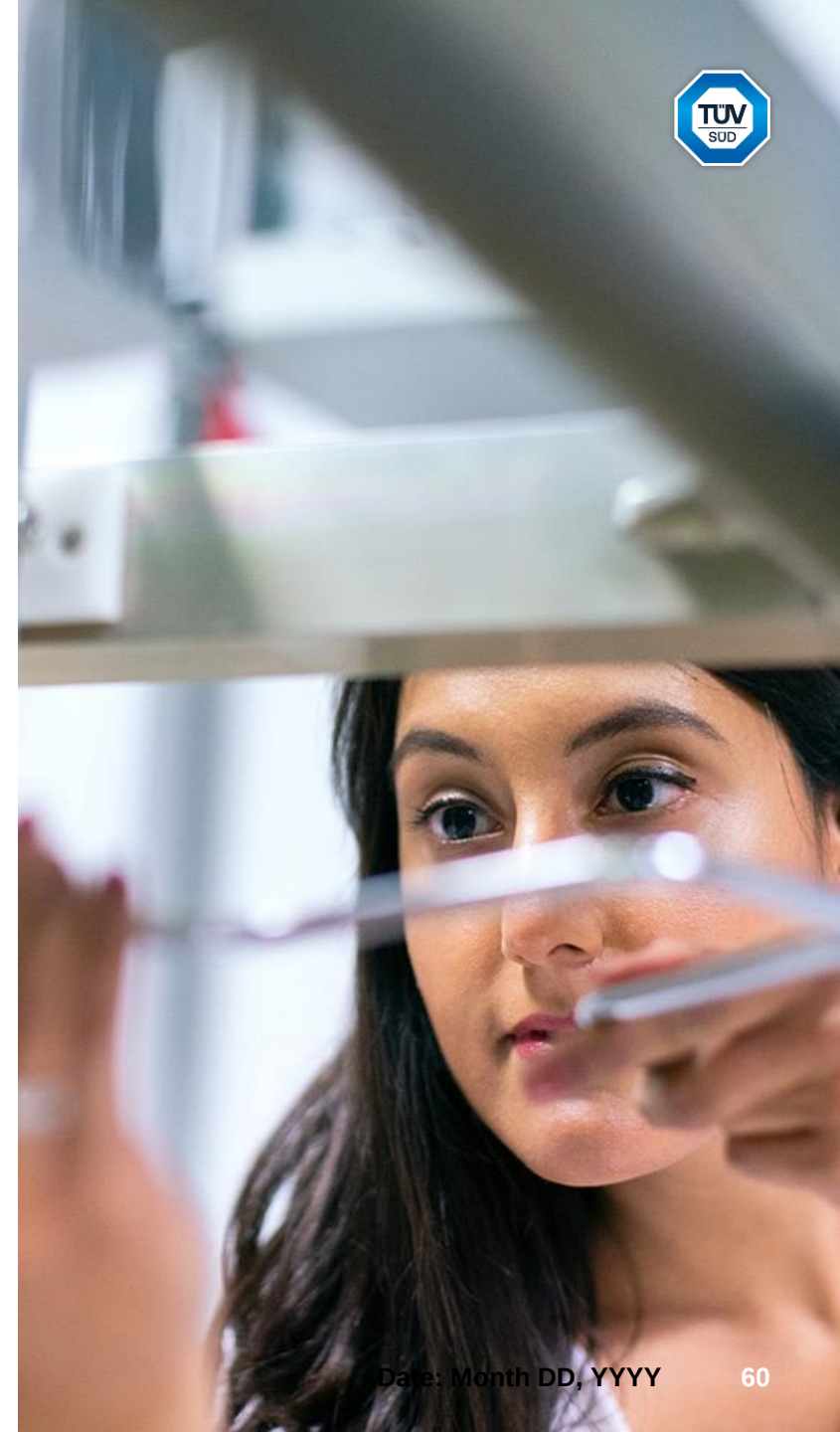
- Oil chem have formed a team to do a PHA of a polystyrene unit. In the past, PHA teams have examined only fire potentials as their basis for considering the risk of chemical releases. The new team has been discussing whether or not to expand their review to include unconfined vapor cloud explosions or other worst-case incidents.
- The team is having trouble reaching a consensus on what to do. Some team members have stated that worst-case incident reviews are a waste of time and money, and that they will only serve to scare the surrounding community into demanding that the plant be shut down.





# Summary

- PHAs are methods to systematically determine process hazards.
- Most PHAs do not examine worst-case scenarios. Experience has shown that these catastrophic events do happen and should be studied in a PHA.
- The subjectivity and experience levels of PHA team members have a large impact on the effectiveness of the team. Worker representatives on PHA teams play a crucial role due to their unique knowledge of process facilities.
- If an employer rejects a recommendation for a PHA, they must document why they did not implement the recommendation.
- Safety information contained in PHA reports should be shared with all employees, contractors and communities who could benefit from receiving this information.



# Exercise 2 - Questions



Q1).....are the first events in an accident sequence, the event or action that sets off a chain reaction.

- A. Propagating events
- B. Initiating Events

Q2).....provides a statistically based quantitative assessment of the probability and consequence of major hazards identified .

- A. PHA
- B. HAZOP
- C. RISK ANALYSIS
- D. RISK ASSESSMENT

# Exercise 2 - Questions



Q3) A PHA is performed by a multidisciplinary team experienced in engineering, operations and maintenance.

A. True

B. False

Q4) .....is different in that the consequences of the error may only become dynamic after a period of time when the condition caused by the original error combines with other errors or system failures to bring about unsafe conditions

A. Active Human Error

B. Latent Human Error



# Exercise 2 - Questions



Q5) ..... Is consider as Process Risk Reduction Strategy.

- A. Operator Control Systems (Alarm , DCS, ESD , F&G)
- B. Mitigation Systems (PSV, Bund, Dike , Flare)
- C. Procedure
- D. Emergency Plans
- E. All of the above

# Exercise 2 - Questions



Q6) .....is the first step in the General PHA Procedure flow Chart

- A. Risk Ranking
- B. Define system or Node
- C. Frequency estimation
- D. Consequence analysis

# Exercise 2 - Questions



Q6) .....is the first step in the General PHA Procedure flow Chart

- A. Risk Ranking
- B. Define system or Node
- C. Frequency estimation
- D. Consequence analysis



# Note



# Any Question?



**Follow us on:**



[tuvsud.com](https://tuvsud.com)  
[info@tuvsud.com](mailto:info@tuvsud.com)

# CERTIFIED PHA - HAZOP LEADER

## HAZOP



01

**Module 1**  
INTRODUCTION

02

**Module 2**  
PROCESS SAFETY MANAGEMENT

03

**Module 3**  
HAZOP

04

**Module 4**  
REHAZOP & LOPA

05

**Module 5**  
Checklists

06

**Module 6**  
WHAT IF & FMEA

07

**Module 7**  
LEADERSHIP

08

**Module 8**  
BOWTIE ANALYSIS



# 3

## HAZOP

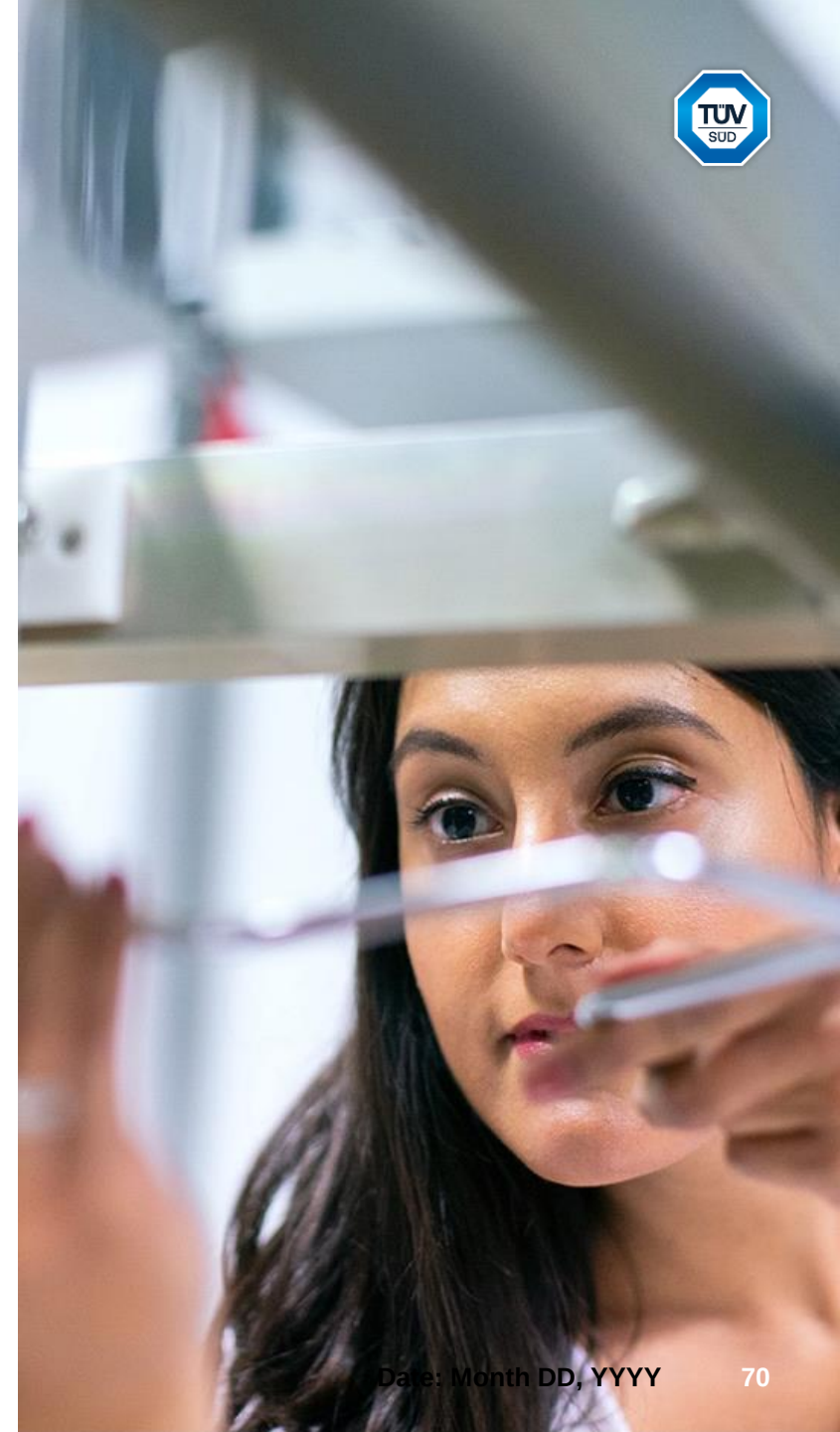


# Module 3

## HAZOP

In this module

- What is a HAZOP?
- People Requirements
- Nodes in HAZOP
- Objectives of HAZOP Analysis
- When HAZOP Study is performed ?
- HAZOP Canvas
- What the Leader Does ?



# What is a HAZOP?



When  
Conduct  
HAZOP

- HAZOP is the most comprehensive PHA at all stages of facility life, from detailed design through construction and routine operation. It identifies operability problems as well as hazards to personnel, the public, company property and the environment.
- A HAZOP is a group technique for identifying hazards and operability problems. It can be applied to operating process plants and to plants in various stages of design
- HAZOP is a highly structured hazards identification tool.
- HAZOP can be used at practically any stage. It is so widely used that almost any form of process hazards analysis is referred to as "HAZOP".
- It is best used as late as possible with a new design, in order to be as complete as possible. With an existing facility it can be used at any time.
- It is extremely basic in its approach and makes practically no assumptions.
- In a HAZOP study, the process under review is first broken down into nodes, which are logical and manageable segments that have a definable design intent. Each node is studied in detail by applying each of the relevant guidewords to design parameters to identify potential cause and consequence of hazards and operability problems.



# What is a HAZOP?



## Potential Causes of Hazards

- Equipment failure, human error, engineering and administrative controls, and external events are all considered as potential causes of hazards. Using a Risk Ranking Matrix, severity and likelihood rankings are estimated and a numerical risk ranking is assigned to each identified hazard.
- Requires considerable amounts of process and safety information.
- Uses systematic, structured examination augmented by creative team thinking.
- Encourages interaction of team members with diverse backgrounds and knowledge.
- Looks at equipment, instrumentation, utilities, human action (routine and nonroutine), building and equipment siting, procedures, and external factors to reveal hazardous situations.
- Ranks identified risks for severity and likelihood
- Can be made applicable to almost any industry, process or system.
- Can be used effectively to perform job task analyses and procedures.
- Makes note of existing safeguards and evaluates them for sufficiency.
- Ensures each recommendation is thoroughly explored because of the diverse team member agendas.
- Can be limited by the assumption the process will be operated as it was designed to operate

# People Requirements



# People Requirements

- Leader experienced in the technique.
- up to eight (maximum) team members with specific knowledge about some aspect of the process being reviewed (too many can slow study and reduce quality).
- example team members:
  - chemical, electrical, mechanical engineering specialists
  - safety specialist
  - vendor representative
  - maintenance personnel and operators
- Comprises a leader who asks questions of the team, a recorder who records the discussion and team members who represent of each of the key disciplines involved in the facility such as:
  - Process design
  - Operations
  - Safety and maintenance





# People Requirements

- The HAZOP team members represent the main disciplines concerned with the design and normal operation of the system such as a process plant
- The team leader and recorder typically are independent of the plant but need to be experienced in the HAZOP technique
- Team size is typically 5-8. Greater numbers reduce the pace and inhibit discussion but with too few members, the team may lack perspective



# Team Leader



- Plan sessions and timetable
- Control discussion
- Limit discussion
- Encourage team to draw conclusion
- Ensure secretary has time for taking note
- Keep team in focus
- Encourage imagination of team members
- Motivate members
- Discourage recriminations
- Judge importance issues
- Always prepare study program in advance.
- Agree on the format or form to be used.
- Prepare follow up procedures.
- Brief members about HAZOP during first meeting.
- Stop the team trying to redesign the process.
- HAZOP is a team exercise. Do not let anybody (including the leader himself to dominate).





# Team Leader

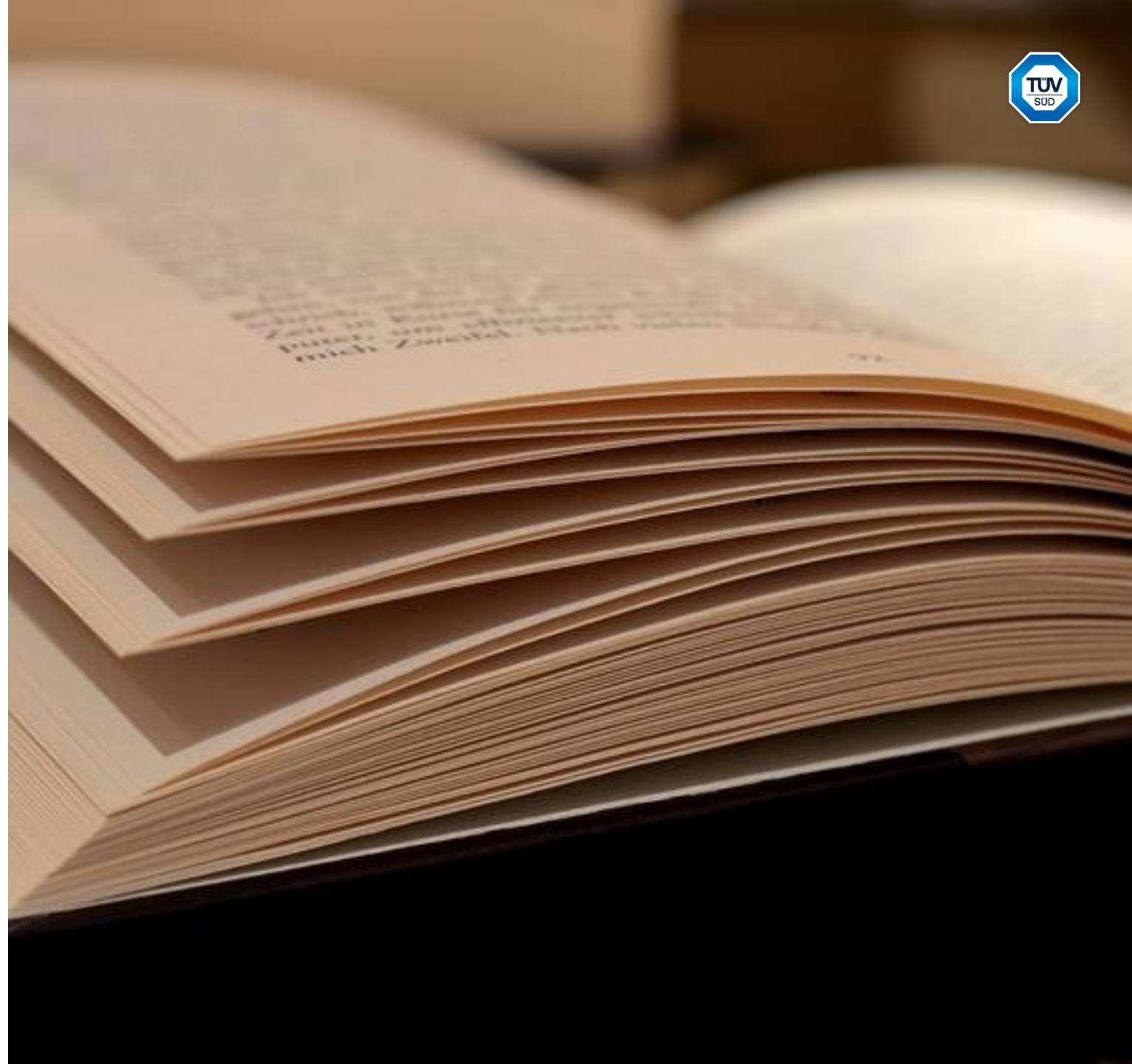
- If conflict arises, handle with care.
- Avoid long discussions by recording areas which need to be resolved outside meeting.
- Leader must be strong, yet diplomatic.
- Speak clearly. Make your point.
- Better have experience working as team member previously.
- Do not skip anything....some time small things may cause big accident.





# HAZOP Secretary

- Take adequate notes
- Record documentations
- Inform leader if more time required in taking notes
- If unclear, check wording before writing
- Produce interim lists of recommendations
- Produce draft report of study
- Check progress of chase action
- Produce final report



# Process Engineer

- Provide a simple description
- Provide design intention for each process unit
- Provide information on process conditions and design conditions





# Mechanical Design Engineer

- Provide specification details
- Provide vendor package details
- Provide equipment and piping layout information





# Instrument Engineer

- Provide details of control philosophy
- Provide interlock and alarm details
- Provide info on shutdown, safety features





# Plant Engineer or Manager

- Provide information on compatibility with any existing adjacent plant
- Provide details of site utilities and services
- Provide (for study on existing plant) any update on maintenance access and modifications





# Shift Operating Engineer or Supervisor

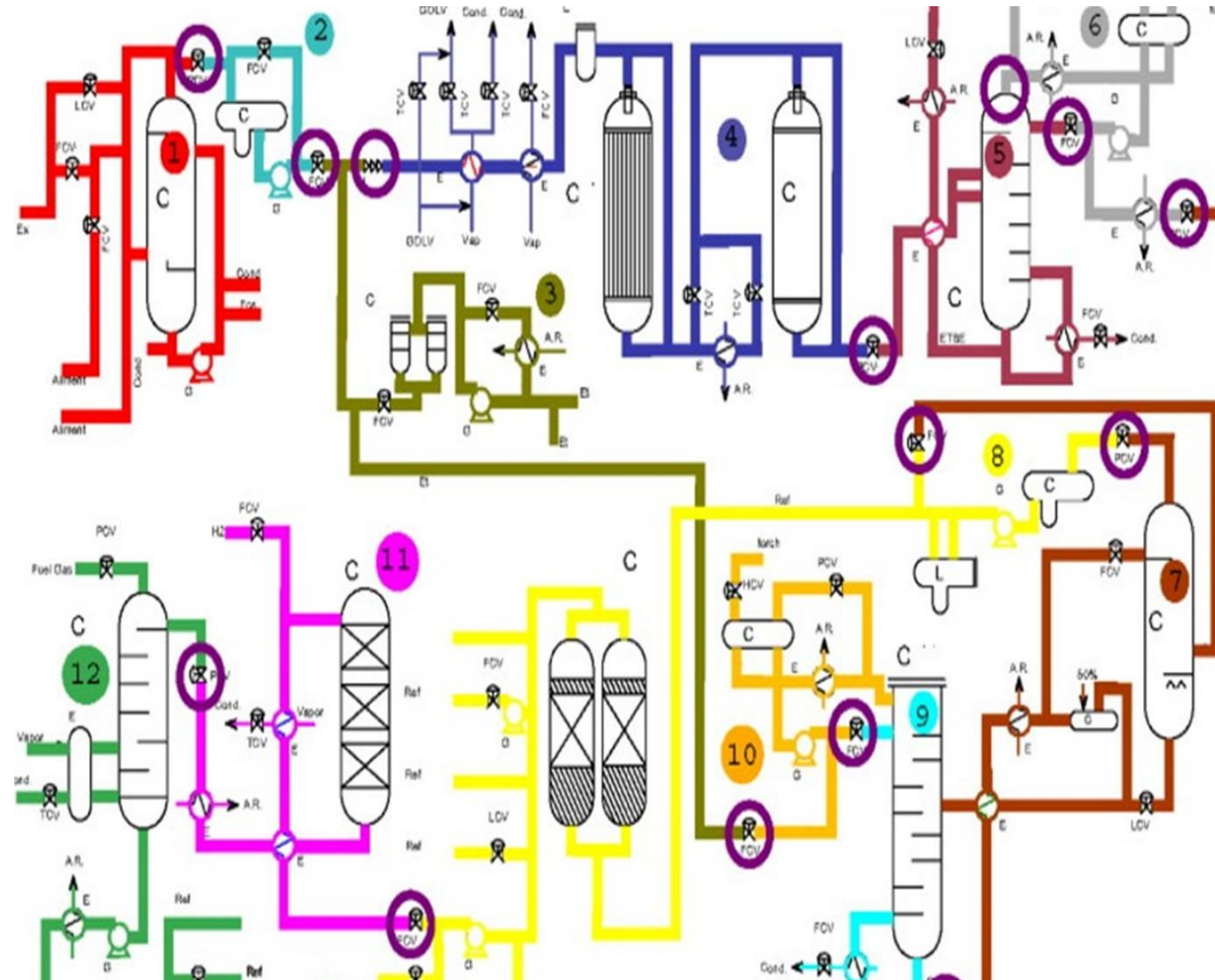
- Provide guidance on control instrumentation integrity from an operating experience view point
- Provide (for study on existing plant) information on plant stability at the specified control parameters
- Provide information on experienced operability deviations of hazard potential





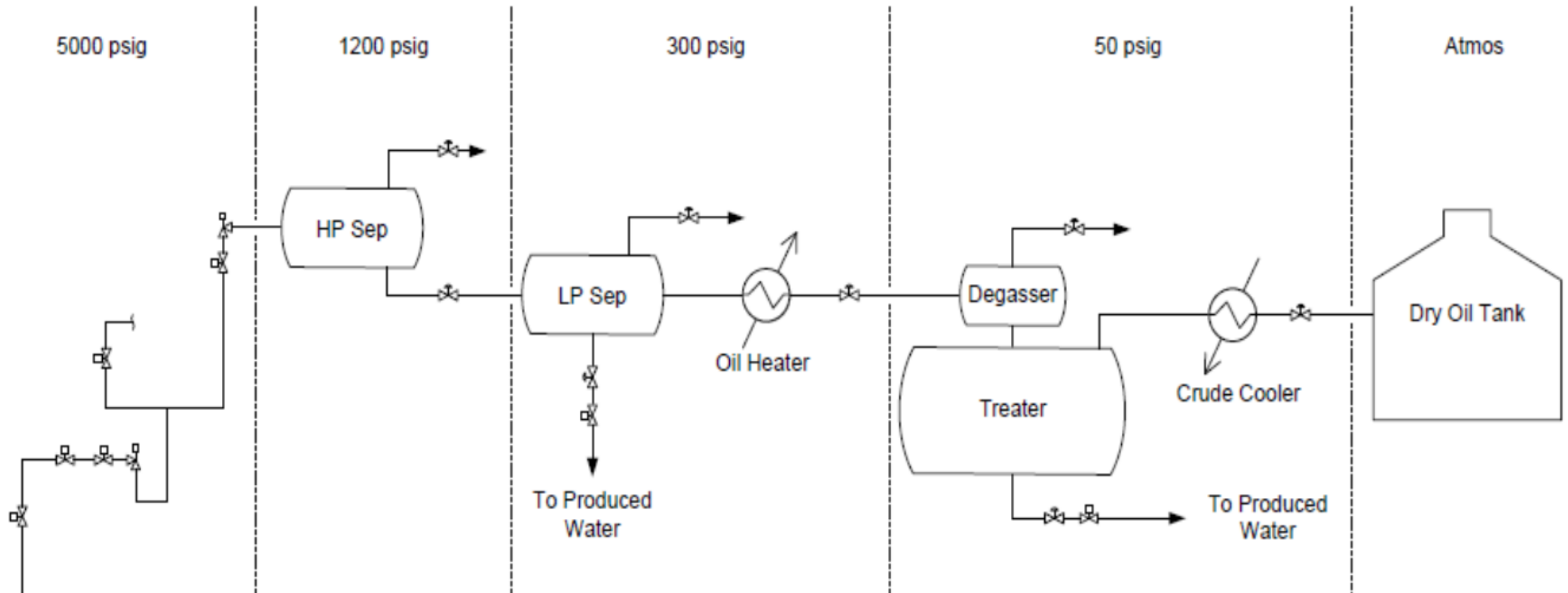
# Nodes in HAZOP

- In a HAZOP Study we take the process plant node by node for more clearance. Nodes Can be
  - Lines
  - Vessels
  - Plant sections
  - Process steps



# Nodes in HAZOP

- Equipment-based nodes (typical HAZOP nodes)
- Stream-based nodes for the FLOW discussions



# Nodes in HAZOP



- A node is typically limited to one major equipment item and associated piping, control systems, safeguarding systems





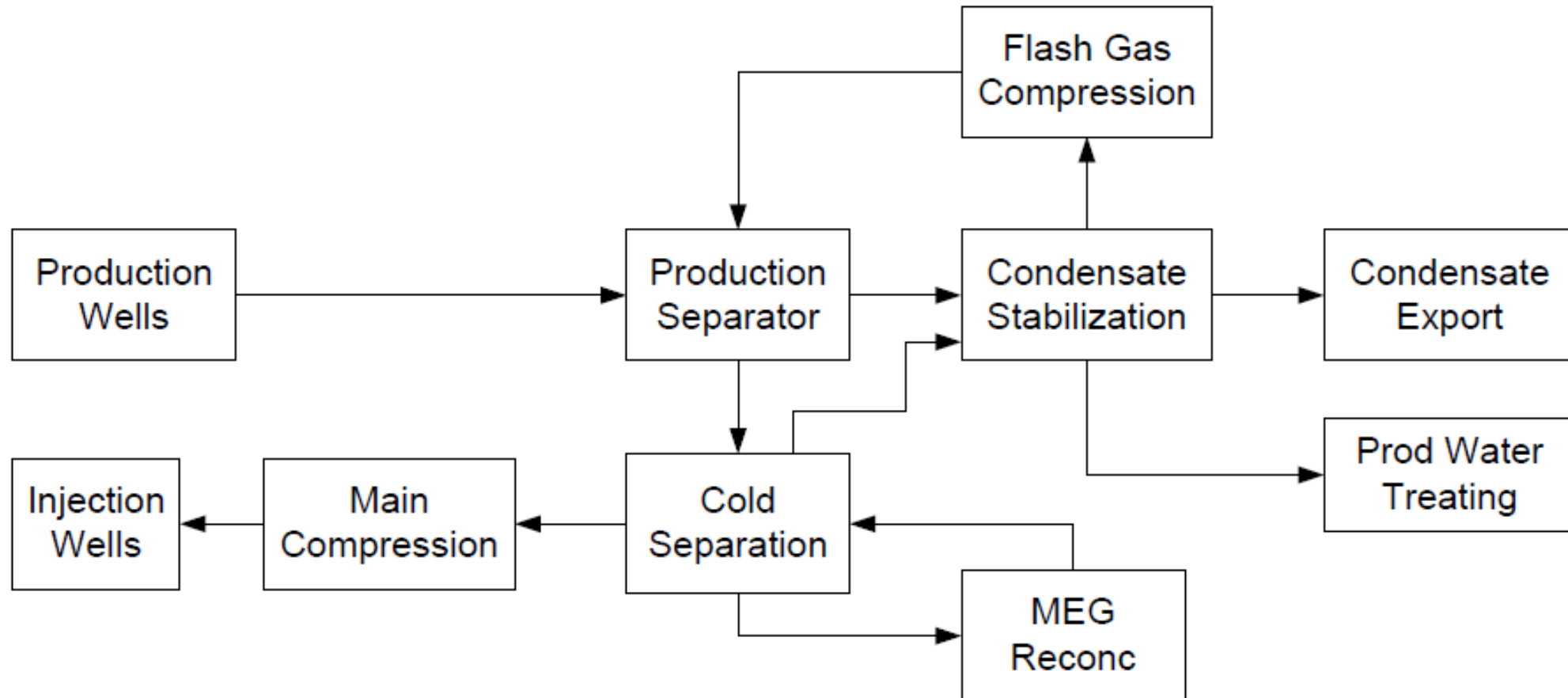
# Stream-based nodes



Base of  
stream-base  
node  
discussions

- Stream-based nodes are based on streams rather than equipment items
- The stream is changed along the way: it is heated and cooled, gas is flashed off, water is separated out, but it is still one 'stream'. Stop the flow anywhere and you stop it everywhere
- The stream-based node solves the tunnel vision problem of small nodes.
- Stream-based nodes are much better for FLOW deviations discussions. Change the flow anywhere in the node and you change it everywhere, or at least everywhere downstream.
- The stream-based node also enables a discussion of operating procedures. We can talk about how the node will be started up, shutdown, commissioned, operated with equipment out-of-service
  - FLOW discussions based on the stream-based nodes.
  - Followed by PRESSURE, TEMPERATURE and LEVEL discussions based on the equipment-based nodes.

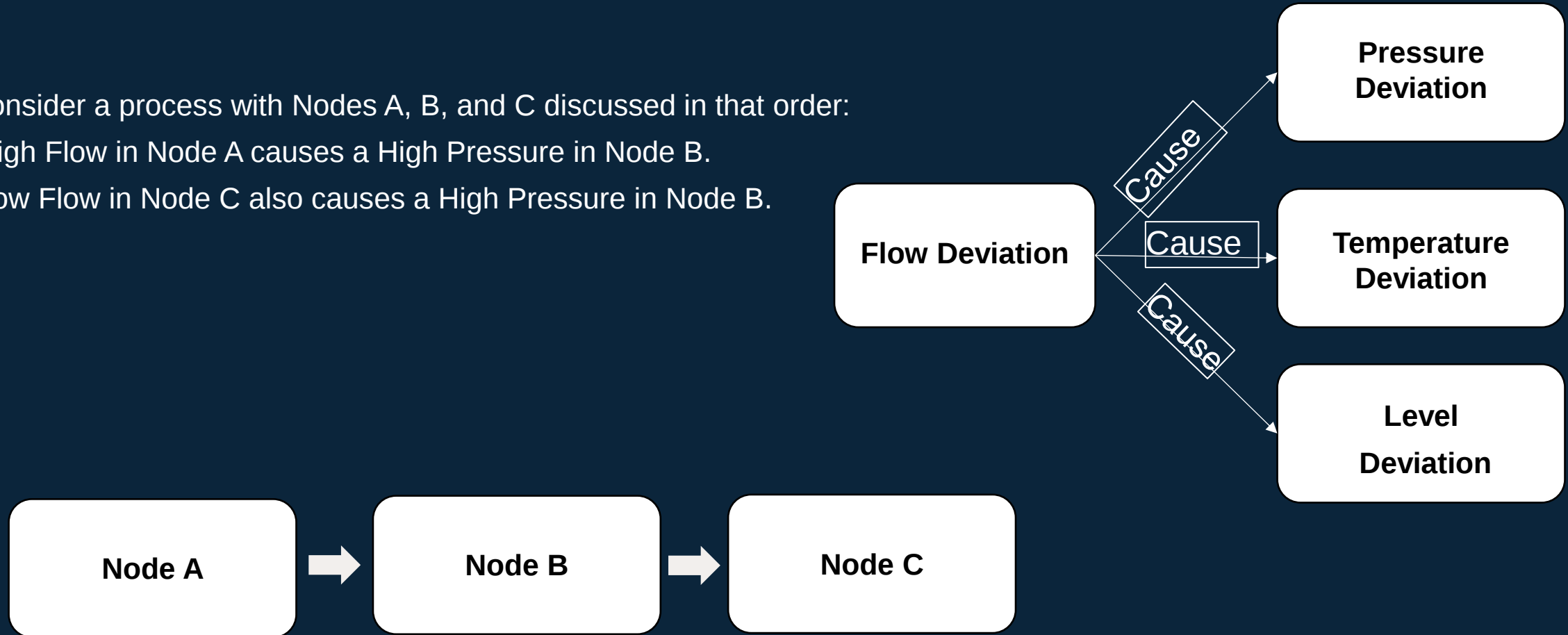
# Identifying Streams



# Guideword Overlap



- Consider a process with Nodes A, B, and C discussed in that order:
- High Flow in Node A causes a High Pressure in Node B.
- Low Flow in Node C also causes a High Pressure in Node B.



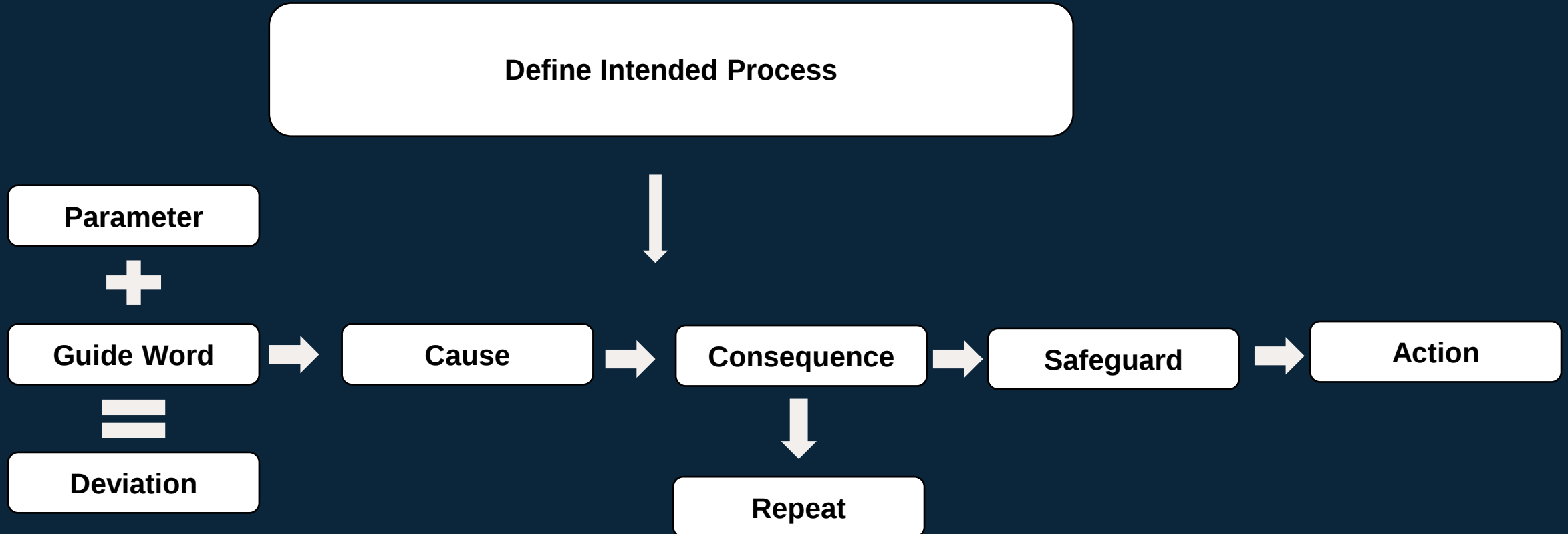


# Objectives of HAZOP Analysis

- to determine if process deviation can lead to undesirable consequences.
- to identify operability problems as well as hazards to personnel, the public, company property and the environment.
- to identify where more research into cause and consequence need to be conducted.
- to recommend changes or improvements to design or operation.



# HAZOP APPROACH





# When

- HAZOP Study is performed when we have a new process plant.
- When we modify an existing plant ( make changes )
- Before start-up
- Once we have at least P&ID Or PFD for the plant
- Every 5 years for operating existing plant





# HAZOP Canvas



- The HAZOP Canvas is a practical way to visual the interworking components of a HAZOP. We believe the HAZOP Canvas offers a simples tool for understanding and
- implementing a HAZOP. The HAOZP canvas comprises of eight building blocks. Each building blocks serve as the foundation to build strong logical arguments for risk-based decisions.
  - NODE
  - DEVIATION
  - CAUSE
  - COSEQUENCE
  - INHERENT RISK
  - SAFEGUARDS
  - OPERTIONAL RISK RANKING
  - RECOMMENDATIONS

| Study Node | Process Parameter | Guide Word | Deviation | Possible Causes | Possible Consequences | Action Required | Responsible | Target Date | Completed Date |
|------------|-------------------|------------|-----------|-----------------|-----------------------|-----------------|-------------|-------------|----------------|
| 1          | 2                 | 3          | 4         | 5               | 6                     | 7               | 8           | 9           | 10             |
|            |                   |            |           |                 |                       |                 |             |             |                |
|            |                   |            |           |                 |                       |                 |             |             |                |
|            |                   |            |           |                 |                       |                 |             |             |                |
|            |                   |            |           |                 |                       |                 |             |             |                |
|            |                   |            |           |                 |                       |                 |             |             |                |
|            |                   |            |           |                 |                       |                 |             |             |                |
|            |                   |            |           |                 |                       |                 |             |             |                |
|            |                   |            |           |                 |                       |                 |             |             |                |
|            |                   |            |           |                 |                       |                 |             |             |                |

# DEVIATION

- Parameter: FLOW
- Design Intent: 20 - 60 m3/hr
- Guide Word Deviation
- More More Flow
- Less Less Flow
- No No Flow
- Reverse Reverse Flow

| Parameters              | Key Word                    | Definition                                                                              |
|-------------------------|-----------------------------|-----------------------------------------------------------------------------------------|
| Flow                    | More<br>No, Less<br>Reverse | Quantitative increase<br>Quantitative decrease (includes no flow)<br>Opposite direction |
| Pressure                | More<br>Less                | More than normal operating<br>Less than normal operating                                |
| Temperature             | More<br>Less                | More than normal<br>Less than normal                                                    |
| Level                   | More<br>Less                | More than normal<br>Less than normal                                                    |
| Composition             | Different from              | Solid or liquids (if applicable)<br>Corrosive<br>Explosive<br>Out of specification      |
| Other                   | Leakage and spillage        | Leakage or release to atmosphere                                                        |
| Utilities               | No, Less                    | Loss of utilities                                                                       |
| Operation & Maintenance | No<br>Other Than            | Maintenance cannot be safely carried out<br>Improper isolation                          |

# DEVIATION

- Parameter: TEMPERATURE
- Design Intent: 120 - 140 °C
- Guide Word Deviations
- More Higher Temperature
- Less Lower Temperature
- No
- Reverse Deviation not meaningful

| Parameters              | Key Word                    | Definition                                                                              |
|-------------------------|-----------------------------|-----------------------------------------------------------------------------------------|
| Flow                    | More<br>No, Less<br>Reverse | Quantitative increase<br>Quantitative decrease (includes no flow)<br>Opposite direction |
| Pressure                | More<br>Less                | More than normal operating<br>Less than normal operating                                |
| Temperature             | More<br>Less                | More than normal<br>Less than normal                                                    |
| Level                   | More<br>Less                | More than normal<br>Less than normal                                                    |
| Composition             | Different from              | Solid or liquids (if applicable)<br>Corrosive<br>Explosive<br>Out of specification      |
| Other                   | Leakage and spillage        | Leakage or release to atmosphere                                                        |
| Utilities               | No, Less                    | Loss of utilities                                                                       |
| Operation & Maintenance | No<br>Other Than            | Maintenance cannot be safely carried out<br>Improper isolation                          |



# DEVIATION

- Parameter: COMPOSITION
- Design Intent: 50 - 60 % Concentration of 'A'
- Guide Word Deviation
- More Higher Concentration
- Less Lower Concentration
- As Well As Impurity
- Other Than Some other material

| Parameters              | Key Word                    | Definition                                                                              |
|-------------------------|-----------------------------|-----------------------------------------------------------------------------------------|
| Flow                    | More<br>No, Less<br>Reverse | Quantitative increase<br>Quantitative decrease (includes no flow)<br>Opposite direction |
| Pressure                | More<br>Less                | More than normal operating<br>Less than normal operating                                |
| Temperature             | More<br>Less                | More than normal<br>Less than normal                                                    |
| Level                   | More<br>Less                | More than normal<br>Less than normal                                                    |
| Composition             | Different from              | Solid or liquids (if applicable)<br>Corrosive<br>Explosive<br>Out of specification      |
| Other                   | Leakage and spillage        | Leakage or release to atmosphere                                                        |
| Utilities               | No, Less                    | Loss of utilities                                                                       |
| Operation & Maintenance | No<br>Other Than            | Maintenance cannot be safely carried out<br>Improper isolation                          |

# CAUSES



- All possible causes for the Deviation are to be listed by the HazOps Team. Examples:
- Deviation : More Flow
- Causes:
  - Control valve open more (malfunction)
  - Multiple pumps in operation.
  - Increase in density.
  - Reduced back pressure.

| Project Name: Biomass: pyrolysis technology |                     |                        |            |                                                                                                                                           | Date: 31/7/15                                                                                                                                                                                                                      |                                                                                                                                                | Page: 2 of 3                         |  |
|---------------------------------------------|---------------------|------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|--|
| Process Equipment (PFD #): R1               |                     |                        |            |                                                                                                                                           |                                                                                                                                                                                                                                    |                                                                                                                                                |                                      |  |
| Section: Pyrolysis                          |                     |                        |            |                                                                                                                                           |                                                                                                                                                                                                                                    |                                                                                                                                                |                                      |  |
| Item                                        | Study Node          | Process Parameters     | Deviations | Possible Causes                                                                                                                           | Possible Consequences                                                                                                                                                                                                              | Action Required                                                                                                                                | Assigned to                          |  |
| 2                                           | Feed Stream (inlet) | Flow of N <sub>2</sub> | No         | 1. Closed outlet valve on FBR<br>2. No reaction/material in FBR<br>3. Vapor steam condensing in previous heat exchanger.                  | • No water condensed or recycled steam shortage in subsequent reactions.<br>• Excess heat retained in, equipment damage.                                                                                                           | 1. Consider a valve that fails open<br>2. Install alarm/sensor                                                                                 | Engineer<br><br>Engineer             |  |
|                                             |                     |                        | Less       | 1.Valve on FBR partly closed<br>2. Some vapor condensing in previous heat exchanger.                                                      | • Not enough water recycled; steam shortage.<br>• Previous HX damaged by condensation.                                                                                                                                             | 1. Consider a valve that fails open.<br>2. Install a flow meter                                                                                | Engineer<br><br>Engineer             |  |
|                                             |                     |                        | More       | 1. More raw material in FBR than expected; more gases evolved as byproducts.<br>2. Higher temperatures lead to volume expansion of gases. | • More water condensed and recycled than needed; extra energy must be supplied.<br>• Condenser experiences a higher pressure.                                                                                                      | 1. Install a flow regulator and flow splitter.<br>2. Design condenser using stronger materials.                                                | Engineer<br><br>Engineer             |  |
|                                             |                     | Temperature            | High       | 1. Not enough cooling water for previous heat exchanger.<br>2. Gas products leaving FBR hotter than expected.                             | • Less water will be condensed, causing a steam shortage.<br>• More water vapor entrained in CO2 stream leaving condenser, which can affect the yield of the pyrolyzer.                                                            | 1. Consider valves that fail open and more powerful pumps.<br>2. Install flow meter.<br>3. Install O <sub>2</sub> flowmeter and regulate T, P. | Engineer<br><br>Engineer<br>Engineer |  |
|                                             |                     |                        | Low        | 1. Too much cooling water in previous heat exchanger.<br>2. High heat loss rates in piping between HX and condenser.                      | • More water condensed and recycled than needed; extra steam results in higher pressures in pipes.<br>• Condensed water leaves condenser at lower temperatures than expected; need more energy to reevaporize water to form steam. | 1. Insulate pipe between previous heat exchanger and condenser.<br>2. Install flow regulator.<br>3. Design larger steam pipes                  | Engineer<br><br>Engineer<br>Engineer |  |
|                                             |                     |                        |            |                                                                                                                                           |                                                                                                                                                                                                                                    |                                                                                                                                                |                                      |  |

# CAUSES



- More Examples:
- Deviation : Less Flow
- Causes:
  - Downstream valve throttled / line blocked.
  - Pump suction strainer fouled / impeller worn out.
  - Outflow thro' safety valve (malfunction).
  - Leakage through heat exchanger tubes.

| Project Name: Biomass: pyrolysis technology |                     |                        |            | Date: 31/7/15                                                                                                                             |                                                                                                                                                                                                                                    | Page: 2 of 3                                                                                                                                   |                                  |
|---------------------------------------------|---------------------|------------------------|------------|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------|
| Process Equipment (PFD #): R1               |                     |                        |            |                                                                                                                                           |                                                                                                                                                                                                                                    |                                                                                                                                                |                                  |
| Section: Pyrolysis                          |                     |                        |            |                                                                                                                                           |                                                                                                                                                                                                                                    |                                                                                                                                                |                                  |
| Item                                        | Study Node          | Process Parameters     | Deviations | Possible Causes                                                                                                                           | Possible Consequences                                                                                                                                                                                                              | Action Required                                                                                                                                | Assigned to                      |
| 2                                           | Feed Stream (inlet) | Flow of N <sub>2</sub> | No         | 1. Closed outlet valve on FBR<br>2. No reaction/material in FBR<br>3. Vapor steam condensing in previous heat exchanger.                  | * No water condensed or recycled steam shortage in subsequent reactions.<br>* Excess heat retained in, equipment damage.                                                                                                           | 1. Consider a valve that fails open<br>2. Install alarm/sensor                                                                                 | Engineer<br>Engineer             |
|                                             |                     |                        | Less       | 1.Valve on FBR partly closed<br>2. Some vapor condensing in previous heat exchanger.                                                      | * Not enough water recycled; steam shortage.<br>* Previous HX damaged by condensation.                                                                                                                                             | 1. Consider a valve that fails open.<br>2. Install a flow meter                                                                                | Engineer<br>Engineer             |
|                                             |                     |                        | More       | 1. More raw material in FBR than expected; more gases evolved as byproducts.<br>2. Higher temperatures lead to volume expansion of gases. | * More water condensed and recycled than needed; extra energy must be supplied.<br>* Condenser experiences a higher pressure.                                                                                                      | 1. Install a flow regulator and flow splitter.<br>2. Design condenser using stronger materials.                                                | Engineer<br>Engineer             |
|                                             |                     | Temperature            | High       | 1. Not enough cooling water for previous heat exchanger.<br>2. Gas products leaving FBR hotter than expected.                             | * Less water will be condensed, causing a steam shortage.<br>* More water vapor entrained in CO2 stream leaving condenser, which can affect the yield of the pyrolyzer.                                                            | 1. Consider valves that fail open and more powerful pumps.<br>2. Install flow meter.<br>3. Install O <sub>2</sub> flowmeter and regulate T, P. | Engineer<br>Engineer<br>Engineer |
|                                             |                     |                        | Low        | 1. Too much cooling water in previous heat exchanger.<br>2. High heat loss rates in piping between HX and condenser.                      | * More water condensed and recycled than needed; extra steam results in higher pressures in pipes.<br>* Condensed water leaves condenser at lower temperatures than expected; need more energy to reevaporize water to form steam. | 1. Insulate pipe between previous heat exchanger and condenser.<br>2. Install flow regulator.<br>3. Design larger steam pipes                  | Engineer<br>Engineer<br>Engineer |



# CAUSES



- More Examples:
- Deviation : Higher Pressure
- Causes:
  - Downstream valve throttled / line blocked.
  - Higher speed of pump / compressor.
  - Higher pressure of steam in reboiler.
  - Less flow of cooling water in condenser.

| Guide Word  | Deviations                            | Possible Causes                                                                                                                                                                                                                                                                                   | Possible Consequences                                                                                                                      |
|-------------|---------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| <b>MORE</b> | More pressure inside the storage tank | Tank exposed to an external heat source<br>Thermal expansion of oil in the storage tank due to fire or strong sunlight<br>Outlet pipe of the storage tank blocked during transfer<br>Failure of the pressure relief valve<br>poor ventilation<br>Failure of the automatic pressure control system | Possible explosion due to rising build up pressure in the tank<br><br>Pressure increases in the tank that could lead to fire and explosion |

# CONSEQUENCES

List the Consequences of each of the Causes (assuming there are no Safeguards).

- Leakage / Toxic Dispersion
- Fire / Explosion Hazard
- (Pool fire, Jet fire, Flash fire, BLEVE, Vapour cloud explosion)
- Accident / injury
- Equipment / property damage
- Production / material loss
- Quality control problem



# SAFEGUARDS

Safeguards protect integrity of the system when deviations may lead to conditions beyond design intentions.

## Types of Safeguards :

- Passive / Inherently Safe.
- Active.
- Procedural.



# SAFEGUARDS

## **Inherently Safe / Passive Safeguards:**

- Design for max. pressure / temperature
- Limited temperature of heating medium
- Limited inventory
- Containment
- Less toxic material used





# SAFEGUARDS

## Active Safeguards:

- Monitoring Instruments / Alarms
- Interlocks
- Emergency Relief
- Inert Blanket / Purge
- Automatic Deluge System



# SAFEGUARDS

## Procedural Safeguards:

- Check Lists
- O&M Manuals / SOP
- Manual Isolation
- Testing / Analysis

## Operation and Maintenance of Pump

### WASA Tube well/Disposal Station



## Operation and Maintenance of Pump

### • Operation of system

- Ensuring effective routine running of system timely and daily.
- Stability
- Efficient
- Safely

### • Maintenance

- Keep of structures/system including planned
- Preventive or Corrective maintenance
- Repair

## Operation and Maintenance plan

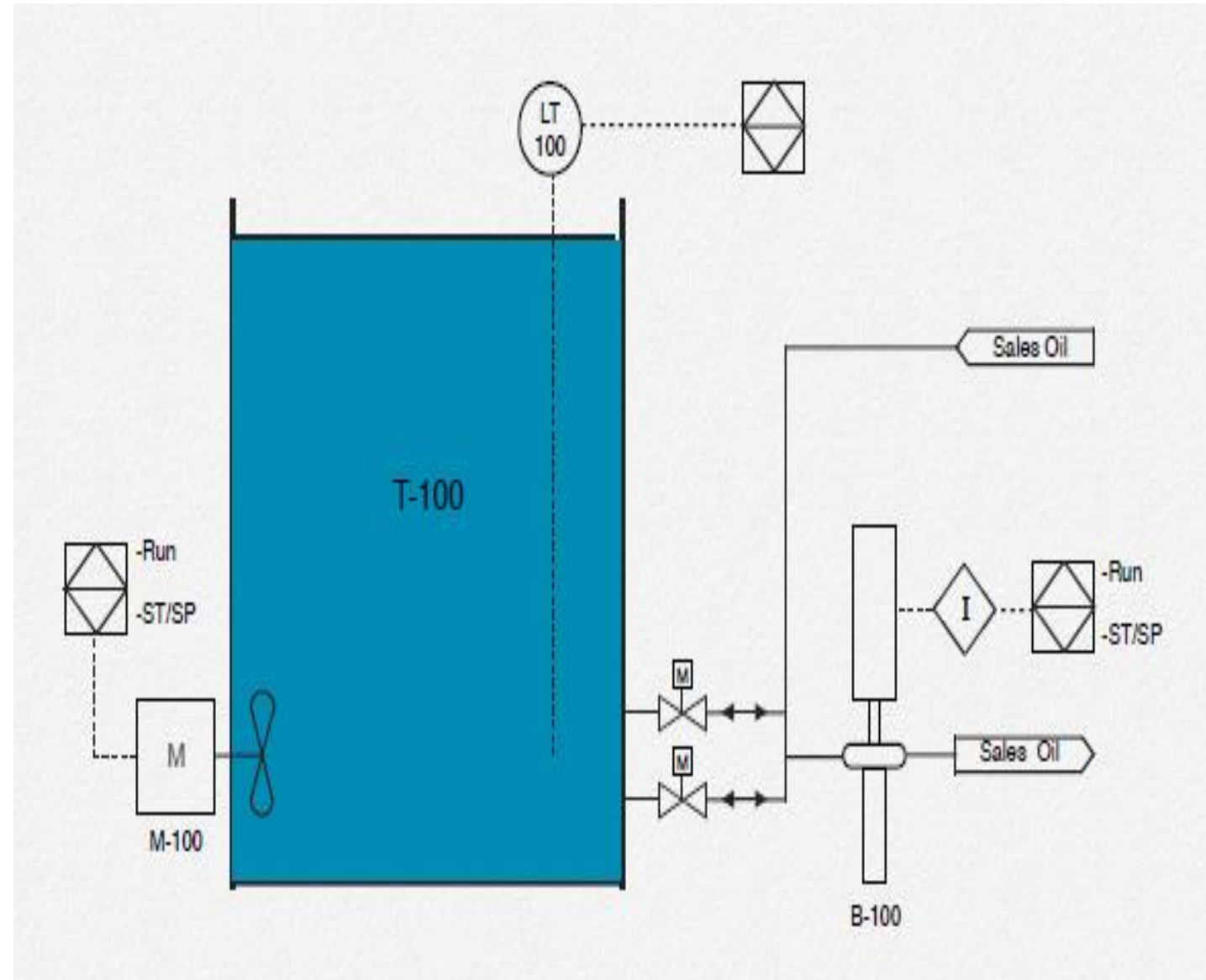
### Operation Record and Manual

- Keep a operational record continuously.
- Prepare a O&M Manual (SOP).



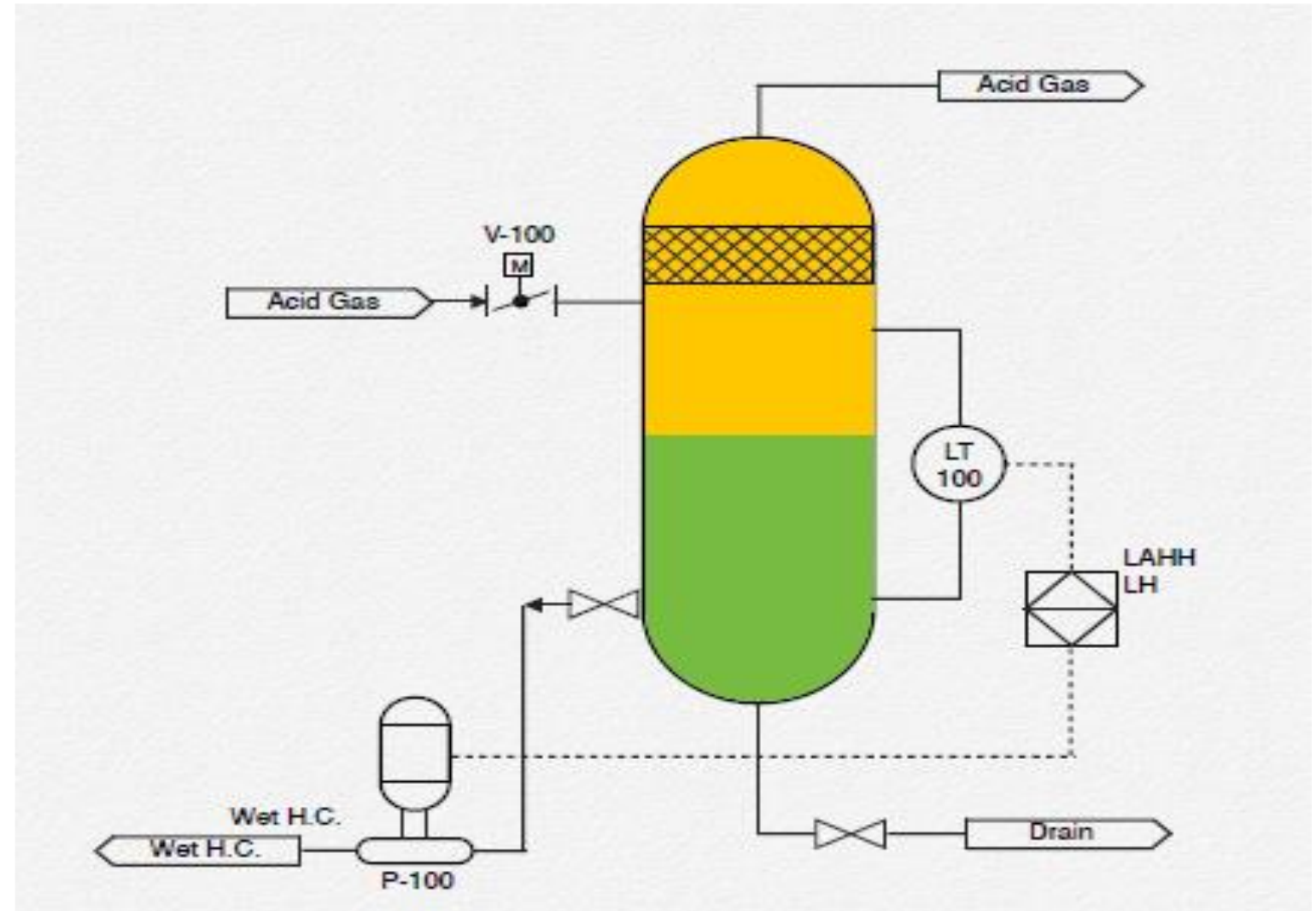
# Examples 1

## Oil Terminal



# Examples 2

## Acid Gas Liquid Separator



# What happens in a HAZOP?

## The plant to be studied

- Is defined at the beginning of the HAZOP typically using a Piping and Instrumentation Diagram to clarify the battery limits and interfaces

## The team operates

- A question and answer approach using guidewords to search for deviations from design intent or failure modes of the plant.





# Preparation

- Preparation includes ensuring the technical drawings such as P&IDs and supplementary information such as data sheets and manuals are complete and up to date
- For an existing plant this means “as built” P&ID are essential; if the plant is under design the latest revisions are required. Working from incomplete or out-of-date documentation is a serious pitfall
- (P&ID) are typically used to define the plant within battery limits

## Supplementary materials

- Process flow sheets
- Equipment specifications & vendor detail drawings
- Piping class and relief valve specifications
- Plot layout and classification
- Operating manuals and emergency shut down procedures



# Before the HAZOP

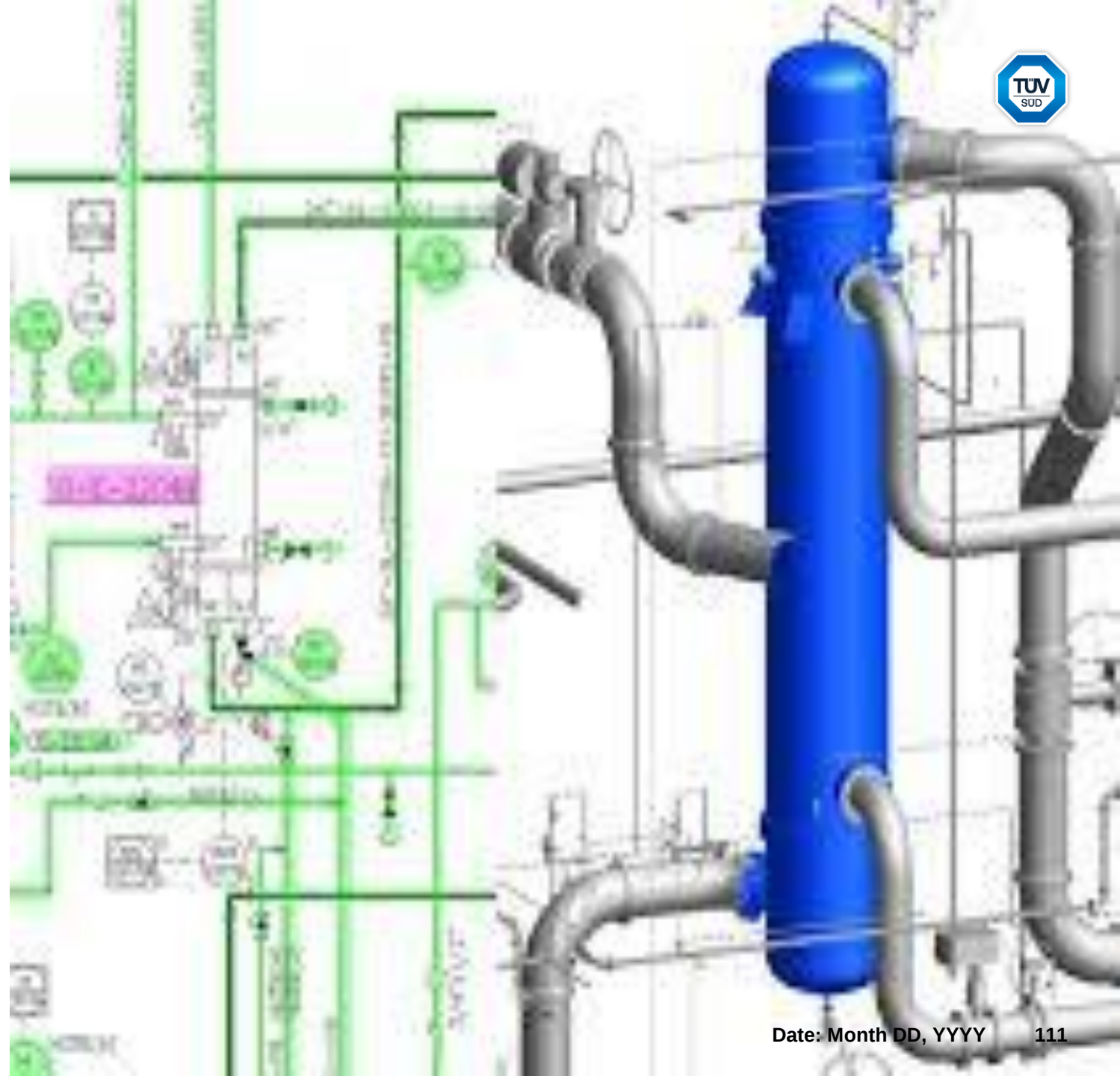
- About a week before the meeting you receive a memorandum describing :
  - The date, time and place for the HAZOP
  - HAZOP study process
  - Study Plan
  - Meeting Rules
- The HAZOP team meets to visit the plant
- For those who do not know the facility this allows a basic description of the process to be provided and gives members a 'mental model' of the plant
- Visit the control room as well as tour outside facilities
- The plan shows the sections of the plant
- The way each section is broken into nodes for HAZOP study
- Which day each node is expected to be examined
- Details of the P&I Drawing related to the node





# Conduct of the HAZOP

- The parameters are the main measurable characteristics of the system such as Flow, Pressure, Temperature and so forth and are applied systematically section by section of the P&ID
- The guidewords are the main deviations such as No, Low, High and so forth and these are interpreted in terms of typical events which cause deviations from design intent in the node under review
- What is the CHAZOP ?





# What is CHAZOP ?



- CHAZOPs are a part of the safety management process that focuses on the potential hazards associated with the operations of the control system exclusive from the function of the underlying processes that they manipulate and maintain.
- CHAZOPs do not only identify hazards related to the integrity of the control system's functions; they also identify hazards related to the operability of the control system. Therefore, the effectiveness of a control system's instrument layout, the material used to explain its functions to relevant personnel, and the notifications and alarms associated with it, are all evaluated as part of a CHAZOP assessment.

| No | Area | System/Components | Scenario/Issues/Concerns | Consequences | Safeguards | Recommendation | Responsibility |
|----|------|-------------------|--------------------------|--------------|------------|----------------|----------------|
|    |      |                   |                          |              |            |                |                |

# Guidewords for Special Situations



- Loss of containment
- Utilities failures
- Environment impact
- Maintenance
- Testing
- Personnel protection
- Plant protection

|            |                                                                                                                  |
|------------|------------------------------------------------------------------------------------------------------------------|
| More       | Quantitative increase                                                                                            |
| Less       | Quantitative decrease                                                                                            |
| As Well As | All the design intention is achieved together with additions                                                     |
| Part of    | Only some of the design intention is achieved                                                                    |
| Reverse    | The logical opposite of the design intention is achieved                                                         |
| Other than | Complete substitution, where no part of the original intention is achieved but something quite different happens |
| Early      | Something happens earlier than expected relative to clock time                                                   |
| Late       | Something happens later than expected relative to clock time                                                     |
| Before     | Something happens before it is expected, relating to order or sequence                                           |
| After      | After Something happens after it is expected, relating to order or sequence                                      |

# Questioning Techniques

- Open questions
- Help person being asked to think – use words how, what and why.
- Closed questions
- To focus on an issue or problem. Start with words who, when, where.
- Required answer yes or no only.
- Question mix
- Mix between open and closed questions.

## Things to avoid

- Ambiguous or vague questions.
- Double parallel/multiple questions.
- Long complicated questions.
- Interrogation type of questions.
- A loaded questions – implied judgement.





# Recommendations

- The recommendations can take the form of open or closed actions. Open actions, calling for further work outside the HAZOP study, will be made for those cases where the situation is complex and the solution is not obvious. Closed actions will be made when the team agree the solution and it is within their level of competency

| Item                                               | Guide Word | Deviation     | Causes                                                                           | Consequences                                                              | Existing Design / Procedural Safeguards                                                    | Recommendations                                                                                                                                          | Action By / Status |
|----------------------------------------------------|------------|---------------|----------------------------------------------------------------------------------|---------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|
| <b>Node 1: Piping from BCD unit and valve box.</b> |            |               |                                                                                  |                                                                           |                                                                                            |                                                                                                                                                          |                    |
| 1.1                                                | No         | No Flow       | Chemical tank is empty.                                                          | No chemical to factory.                                                   | Low liquid level indication at BCD unit only.                                              | Add demand indicator at tool communicating with BCD unit. Install auto-switchover at LL indication and change to more reliable level sensing technology. | George / Open      |
| 1.2                                                | Low        | Low Pressure  | Pipe or fitting leak.                                                            | Inadequate delivery to factory. Personnel injury during repair operation. | Leak detection in valve box and piping is in secondary containment.                        | Currently there is not ability to isolate VB for repair. Add bypass loop at each VB.                                                                     | Steve / Open       |
| <b>Node 2: BCD pump and holding tanks.</b>         |            |               |                                                                                  |                                                                           |                                                                                            |                                                                                                                                                          |                    |
| 2.1                                                | No         | No Flow       | Primary pump fails.                                                              | No chemical to factory.                                                   | Pump MTBF rated at 10K hours                                                               | Consider second pump in standby or on the shelf spare. Conduct predictive maintenance via bearing heat sensing or excess current detection.              | Joe / Open         |
| 2.2                                                | No         | No Level      | Auto-switchover fails when primary tank is empty.                                | No chemical to factory.                                                   | Low-low level sensor will alarm, indicating trouble with switchover, or empty second tank. | None.                                                                                                                                                    | Closed             |
| 2.3                                                | Low        | Flow or Level | Same as No Flow or Level.                                                        |                                                                           |                                                                                            |                                                                                                                                                          |                    |
| 2.4                                                | High       | High Level    | Drawing from both tanks during switchover lag cycle (during low factory demand). | Overfill / overpressure of secondary tank.                                | Rupture disk on tanks.                                                                     | Eliminate or shorten switchover lag time. Plumb rupture disk to a safe location.                                                                         | Jim / Open         |

# HAZOP is **not**

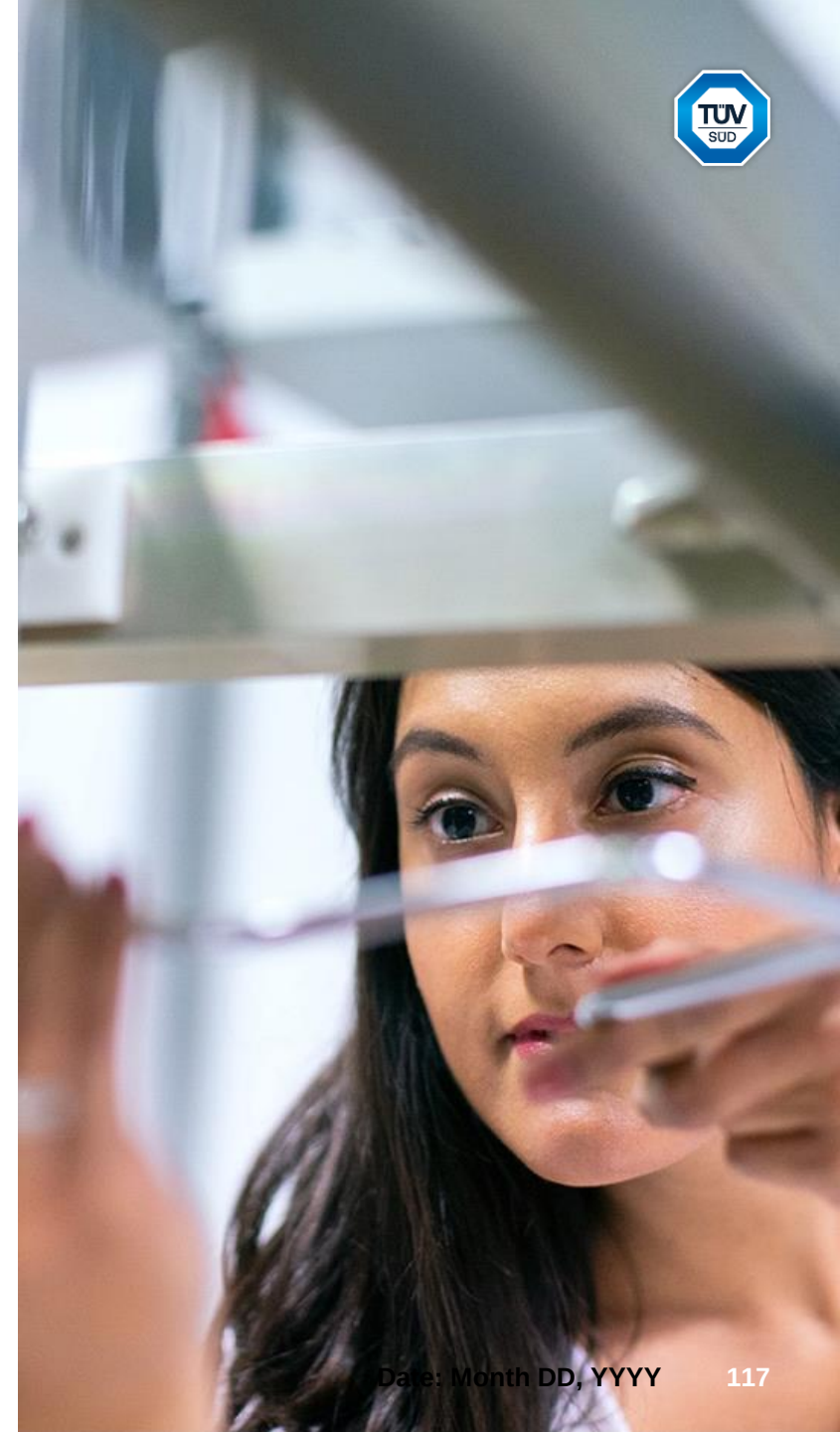


- A Design Review – It should not be regarded as a review to catch bad engineering design.
- A Check of the Quality of a Design – This is the Q.A. function within each department.
- A Check of Compliance to Codes and Standards – This is also a departmental responsibility.
- A Quantitative Risk Analysis – HAZOP may identify the need for QRA or other studies. Risk ranking by coarse probability and consequence evaluation is the limit of the team's role.
- • An End in Itself – In the past, some people have maintained that “if you have had a successful HAZOP study your responsibility for operating safety is completed”-

# Summary

What we have learned in the module

- What is the HAZOP ?
- What is the CHAZOP ?
- When HAZOP Study is performed ?
- Objectives of HAZOP Analysis
- Understand HAZOP APPROACH





# Exercise 3 - Questions



Q1) HAZOP is?

- A. Hazard and operability studies
- B. HAZID and operability studies
- C. Hazard material and operate studies
- D. Hazard and onshore Process for studies

# Exercise 3 - Questions



Q2) Identify sections that is/are not available in HAZOP study form

- A. Deviation
- B. Consequence
- C. Guide words
- D. Cause
- E. None of above(all included)

# Exercise 3 - Questions



Q3) Choose detailed information on the process must be available in order to perform HAZOP analysis

- A. Process flow diagrams (PFDs)
- B. Process description
- C. (P&IDs) diagrams
- D. Detailed equipment specifications
- E. Materials of construction
- F. Mass and energy balances



# Exercise 3 - Questions



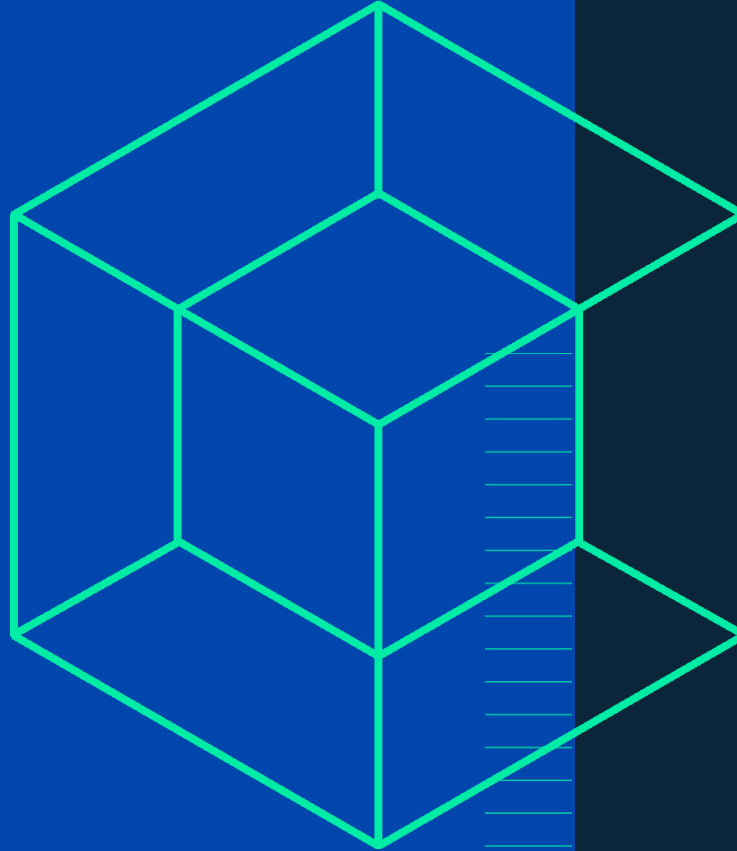
Q4) What is the Purpose of the HAZOP? (Select 3 Answers that apply)

- A. To Propose recommendations
- B. To Provide an alternative to PHA
- C. To Identify Safeguards
- D. To make cost benefit analysis
- E. To Perform Quality Assurance
- F. To Identify Potentially hazard scenario

# Note



# Any Question?



**Follow us on:**



[tuvsud.com](https://tuvsud.com)  
[info@tuvsud.com](mailto:info@tuvsud.com)



# CERTIFIED PHA - HAZOP LEADER

## REHAZOP & LOPA



01

**Module 1**  
INTRODUCTION

02

**Module 2**  
PROCESS SAFETY MANAGEMENT

03

**Module 3**  
HAZOP

04

**Module 4**  
REHAZOP & LOPA

05

**Module 5**  
Checklists

06

**Module 6**  
WHAT IF & FMEA

07

**Module 7**  
LEADERSHIP

08

**Module 8**  
BOWTIE ANALYSIS

# 4

## REHAZOP & LOPA

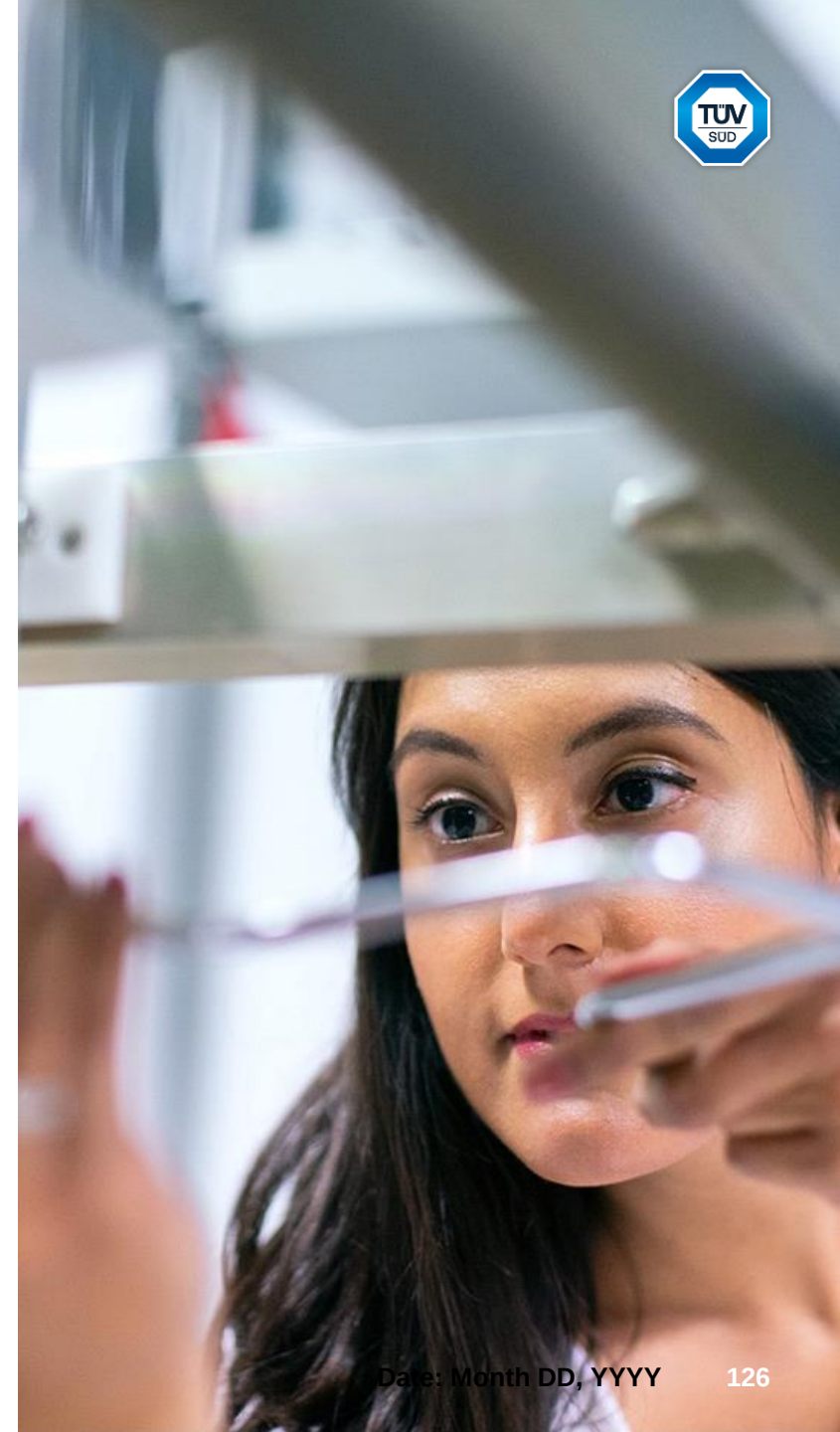


# Module 4

## REHAZOP & LOPA

In this module

- Points to be considered during ReHAZOPs
- Remote HAZOPing
- LOPA
- HAZOP/LOPA
- HAZOP CHARTER
- HAZOP TOR
- Time Required
- Ground Rules





# Points to be considered during ReHAZOPs

- Plant modifications
- Changes in operating Conditions
- Different start up/ shut down sequences
- Changes in manning levels/locations
- Failure to close out actions and validate their completion.
- Degradation of plant integrity or performance
- Changes in standards
- New corporate requirements
- Plant incidents
- Increased awareness of due to operating experience
- Maintenance record
- Safeguards Conditions
- Documents updates and changes
- Plant outages and shutdowns
- Upsets in the process



# Remote HAZOPing

- The COVID-19 pandemic has changed HAZOPing remotely from being a rare occurrence to being common almost overnight.
- One wonders whether this might become more common in the future, either for health reasons or to avoid the costs/time associated with traveling to a HAZOP on the other side of the country or planet.





# What is LOPA ?

- Define the unwanted Impact
- Determine the initiating events and their Frequency
- Determine any Conditional Modifiers or Enabling Events
- Determine the Independent layers of protection (IPL) & their PFD
- Determine any Mitigation Factors to be considered as IPLs & their PFD
- Calculate the resultant frequency of the unwanted impact





# LOPA Worksheet



|                                                          |    |                                          |  |  |
|----------------------------------------------------------|----|------------------------------------------|--|--|
|                                                          | 1  | Impact Event                             |  |  |
| Likelihood are event/year and protection are PFD Average | 2  | Severity Level                           |  |  |
|                                                          | 3  | Initiating Cause                         |  |  |
|                                                          | 4  | Initiation Likelihood                    |  |  |
| Protection & Mitigation Layers                           | 5  | General Design                           |  |  |
|                                                          |    | Control System                           |  |  |
|                                                          |    | Independent Alarm                        |  |  |
|                                                          | 6  | Additional Mitigation, restricted access |  |  |
|                                                          | 7  | Additional Mitigation                    |  |  |
|                                                          | 8  | Intermediate Event Likelihood            |  |  |
|                                                          | 9  | PFDavg required                          |  |  |
|                                                          | 10 | Tolerable Mitigated Event Likelihood     |  |  |
|                                                          | 11 | Notes                                    |  |  |

# Step 1

## Unwanted Impact & Initiating Cause

- The HAZOP is reviewed to identify all cause / consequence pairs which have a SIF included in the safeguards for the hazard scenario
- The Impact event description is the HAZOP Consequence for the hazard scenario under review
- Initiating Cause description is the HAZOP Cause for the hazard scenario under review
- These two descriptions are entered into the LOPA record sheet



|                                                          |    |                                          |
|----------------------------------------------------------|----|------------------------------------------|
|                                                          | 1  | Impact Event                             |
| Likelihood are event/year and protection are PFD Average | 2  | Severity Level                           |
|                                                          | 3  | Initiating Cause                         |
|                                                          | 4  | Initiation Likelihood                    |
| Protection & Mitigation Layers                           | 5  | General Design                           |
|                                                          |    | Control System                           |
|                                                          |    | Independent Alarm                        |
|                                                          | 6  | Additional Mitigation, restricted access |
|                                                          | 7  | Additional Mitigation                    |
|                                                          | 8  | Intermediate Event Likelihood            |
|                                                          | 9  | PFDavg required                          |
|                                                          | 10 | Tolerable Mitigated Event Likelihood     |
|                                                          | 11 | Notes                                    |

# Step 2

## Initiating events –(Cause from HAZOP)



| Initiating Cause                                                           | Initiating Likelihood per/yr | Initiating Likelihood Comment                                   |
|----------------------------------------------------------------------------|------------------------------|-----------------------------------------------------------------|
| Piping failure (Full breach) per 100m length                               | See comment                  | $1 \times 10^{-5}$ /year per 100m length                        |
| Pressure vessel residual failure                                           | 1.0E-06                      | Based on vessel failure                                         |
| Atmospheric Tank failure                                                   | 1.0E-03                      | Based on vessel failure                                         |
| Failure of control system                                                  | 0.1                          | Based on control system failure                                 |
| Control valve                                                              | 0.02                         | Failure to regulate                                             |
| ESD valve                                                                  | 0.04                         | Spurious operation of ESD ball valve                            |
| Safety valve opens spuriously                                              | 0.01                         | Spurious operation of safety valve                              |
| Pump trips                                                                 | 0.04                         | Based on pump spurious stop                                     |
| Operator Error (routine task with written procedure)                       | See comment                  | 0.1 per opportunity                                             |
| Operator Error infrequent task with written procedure)                     | See comment                  | 0.01 per opportunity                                            |
| Major internal leakage/tube failure within a shell and tube heat exchanger | 0.01                         | Selected frequency assumes that exchanger is inspected annually |



# Step 3

## Conditional Modifiers

Use of conditional modifiers can be contentious they must be specific to the site under assessment and require to be determined by analysis. Typical conditional modifiers are:

- Probability of ignition
- Probability of exposure
- Probability of Injury / Fatality
- Metrological
- Probability of explosion after ignition
- Time at Risk



# Step 4

## Identification of IPLs



- Identify BPCS protective function, If any
- List any Alarms and the operator response time and action (EEMUA 191) (written procedure required and auditable training)
- Record qualifying relief devices as preventive functions
- Document Other Potential Safety Related Systems
- Human Intervention
- Machine Protection Systems
- Hydraulic / Pneumatic / Mechanical

|                                                          |    |                                          |
|----------------------------------------------------------|----|------------------------------------------|
|                                                          | 1  | Impact Event                             |
| Likelihood are event/year and protection are PFD Average | 2  | Severity Level                           |
|                                                          | 3  | Initiating Cause                         |
|                                                          | 4  | Initiation Likelihood                    |
| Protection & Mitigation Layers                           | 5  | General Design                           |
|                                                          |    | Control System                           |
|                                                          |    | Independent Alarm                        |
|                                                          | 6  | Additional Mitigation, restricted access |
|                                                          | 7  | Additional Mitigation                    |
|                                                          | 8  | Intermediate Event Likelihood            |
|                                                          | 9  | PFDavg required                          |
|                                                          | 10 | Tolerable Mitigated Event Likelihood     |
|                                                          | 11 | Notes                                    |

# Step 5

## Mitigation



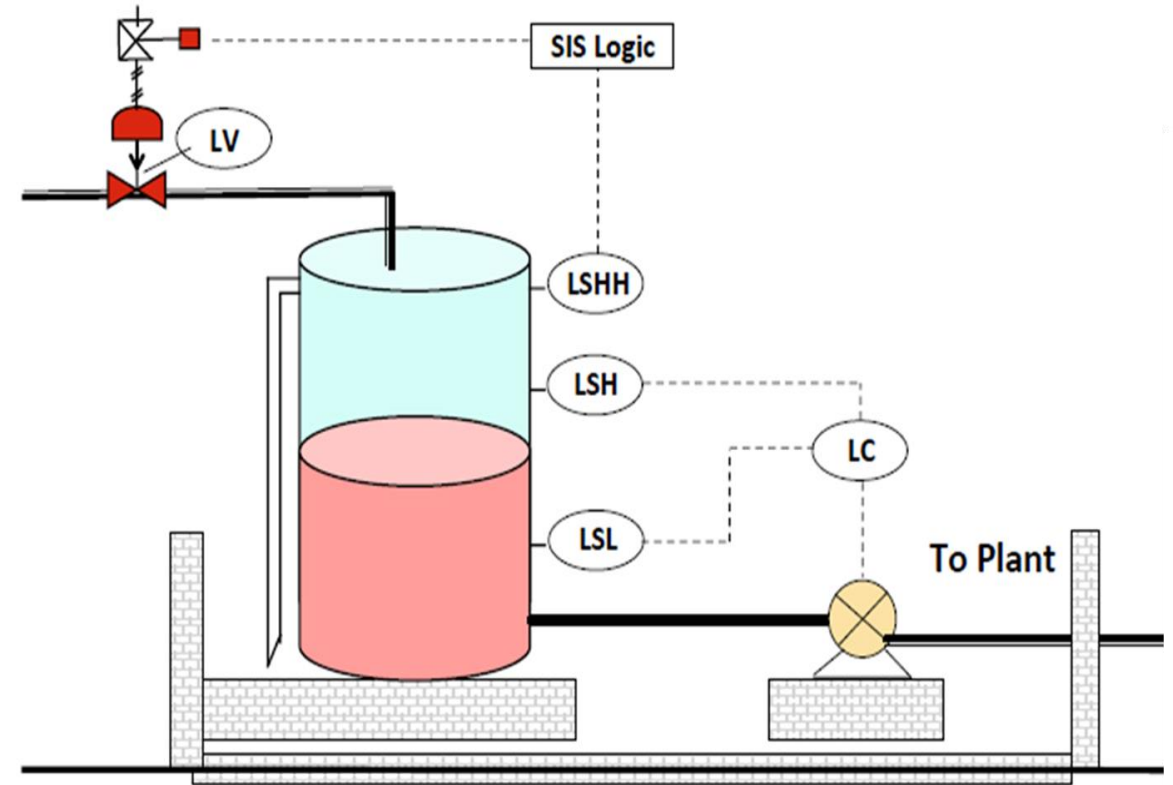
- Fire and Gas Systems
- Relief devices
- Flares
- Containment – Primary / Secondary / Tertiary
- Other Safety Related Protection Systems
- Explosive Relief

|                                                          |    |                                          |
|----------------------------------------------------------|----|------------------------------------------|
|                                                          | 1  | Impact Event                             |
| Likelihood are event/year and protection are PFD Average | 2  | Severity Level                           |
|                                                          | 3  | Initiating Cause                         |
|                                                          | 4  | Initiation Likelihood                    |
| Protection & Mitigation Layers                           | 5  | General Design                           |
|                                                          |    | Control System                           |
|                                                          |    | Independent Alarm                        |
|                                                          | 6  | Additional Mitigation, restricted access |
|                                                          | 7  | Additional Mitigation                    |
|                                                          | 8  | Intermediate Event Likelihood            |
|                                                          | 9  | PFDavg required                          |
|                                                          | 10 | Tolerable Mitigated Event Likelihood     |
|                                                          | 11 | Notes                                    |



# Exercise 1

- This practical exercise requires participants to determine the required RRF of a proposed safety-instrumented system using the basic principles and LOPA parameters described in this module
- A Tank Overfill hazard has identified by the HAZOP team, two causes have been identified:
- Pump failure: 2.0 per year
- Level Control Failure: 0.1 per year
- Determine the required target RRF for personnel safety of the High Level Shut Off to the tank if the tolerable risk for the hazard is  $1.0E-05$



# Exercise 2

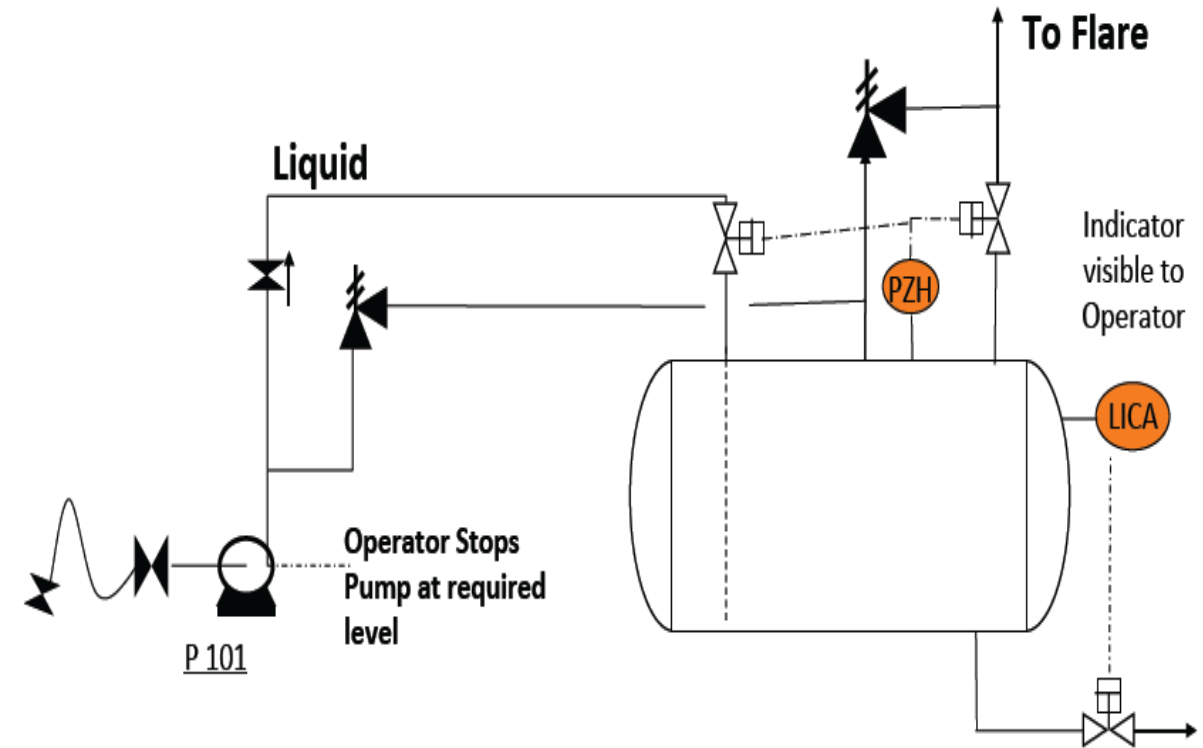


Liquid is transferred manually to a holding tank before delivery to the plant, the operator must stop the pump at 75% Tank Level. A Tank Over pressurization hazard has been identified by the

- HAZOP team, two causes have been identified:
- Operator fails to stop pump : 0.1 per year
- Level Control Failure: 0.1 per year

Determine the required target RRF for personnel safety of the High Pressure Vent SIF to Flare

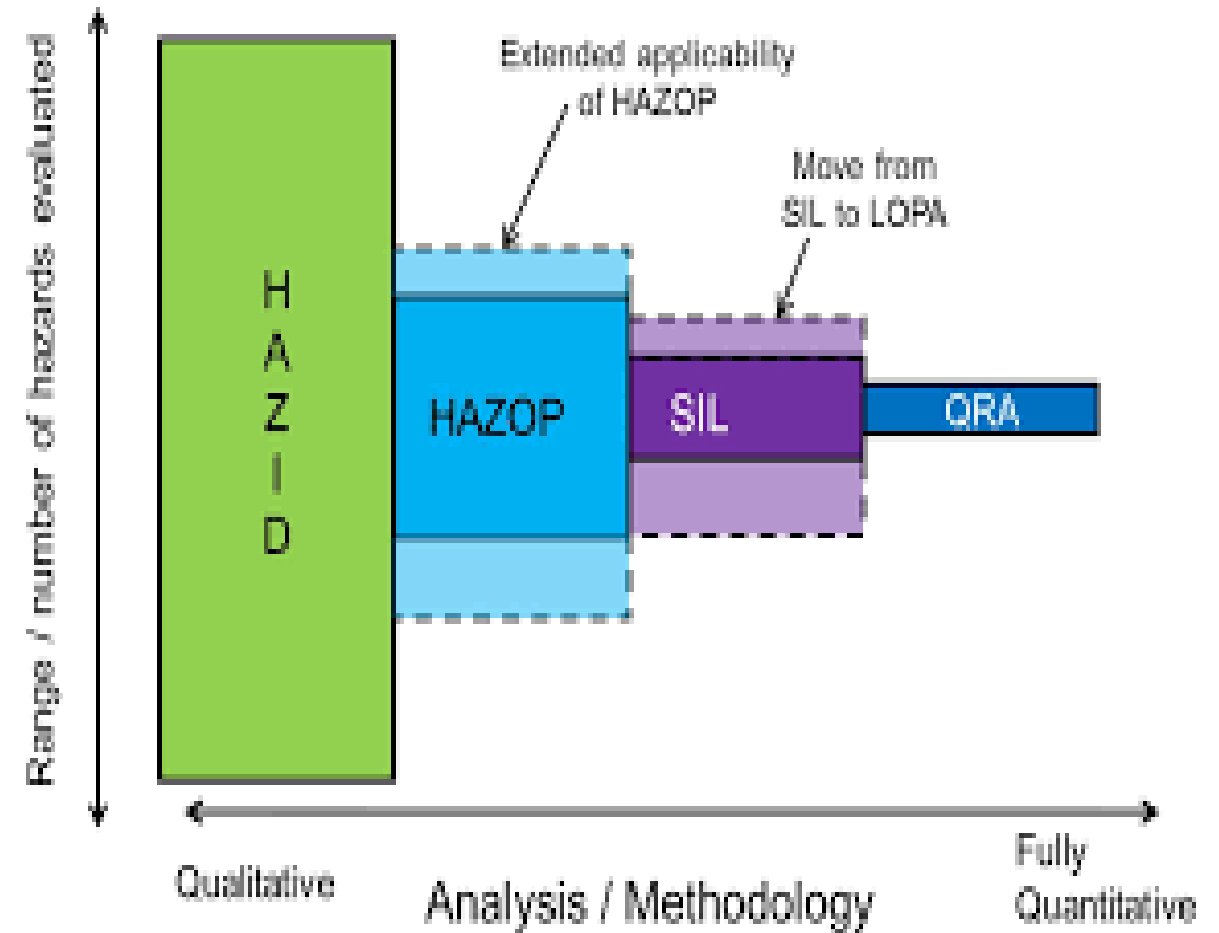
- The tolerable risk for the hazard is  $1.0E-05$
- The Holding tank has a relief valve installed which is sized for full flow and vented to Flare
- The process design is not considered to be fit for purpose



# HAZOP/LOPA



The requirement was for LOPA to be carried following completion of the HAZOP studies. In reality there needed to be a screening exercise following the HAZOP study to decide which events needed to be taken forward to the LOPA study, to exclude events where LOPA was not appropriate





# Where LOPA may **not** be appropriate ?

- Low severity events
- Domino events
- Integrity management issues
- Design errors
- Events initiated by external factors

# Taking credit for HAZOP safeguards

- The LOPA process requires identification of the relevant Independent Protective Layers (IPL) for which risk reduction credit can be taken, and then assigning a PFD value based on either generic values from the company guidance or alternatively based on operating experience
- Does the safeguard prevent the event escalating to the LOPA scenario under review. There were examples where safeguards listed in the HAZOP prevented some consequences being realized but not the hazardous event being assessed in the LOPA. ?
- Is the safeguard fully independent of the initiating cause and all the other IPL ?
- Can a reliability figure be assigned to the IPL, generally this required the IPL to be a registered risk reduction feature that undergoes routine auditing, inspection and/or testing to ensure that the functionality is maintained. For example, if reverse flow is to be prevented by a non-return valve, in order to take risk reduction credit this must be registered as a safety-related device and included on a PM schedule
- A general observation from this process was how many of the HAZOP safeguards did not pass the test to become an IPL, particularly alarms on the DCS due to lack of independence from the controls or not being managed as a 'Safety Related Alarm'. This could lead to a false sense of security following the HAZOP that there are many safeguards and therefore the risk must be low.



# Taking credit for HAZOP safeguards



- Objectives
- Background
- HAZOP Approach and Key Activities
- Deliverables
- HAZOP Methodology / Activities
- HAZOP Team

## **HAZOP Objective**

- A hazard and operability study (or HAZOP) is a systematic, critical examination by a team of the engineering and operating intentions of a process to assess the hazard potential of mal-operation or mal-function of individual items of equipment and the consequential effects on the facility as a whole.
- The HAZOP technique was initially developed to analyze chemical process systems, but has later been extended to other types of systems and also to complex operations and to software systems.



# HAZOP TOR

- Scope and Boundaries
- Schedule
- Roles and Responsibilities
- Data Requirements
- HAZOP Methodology / Activities
- RISK MATRIX



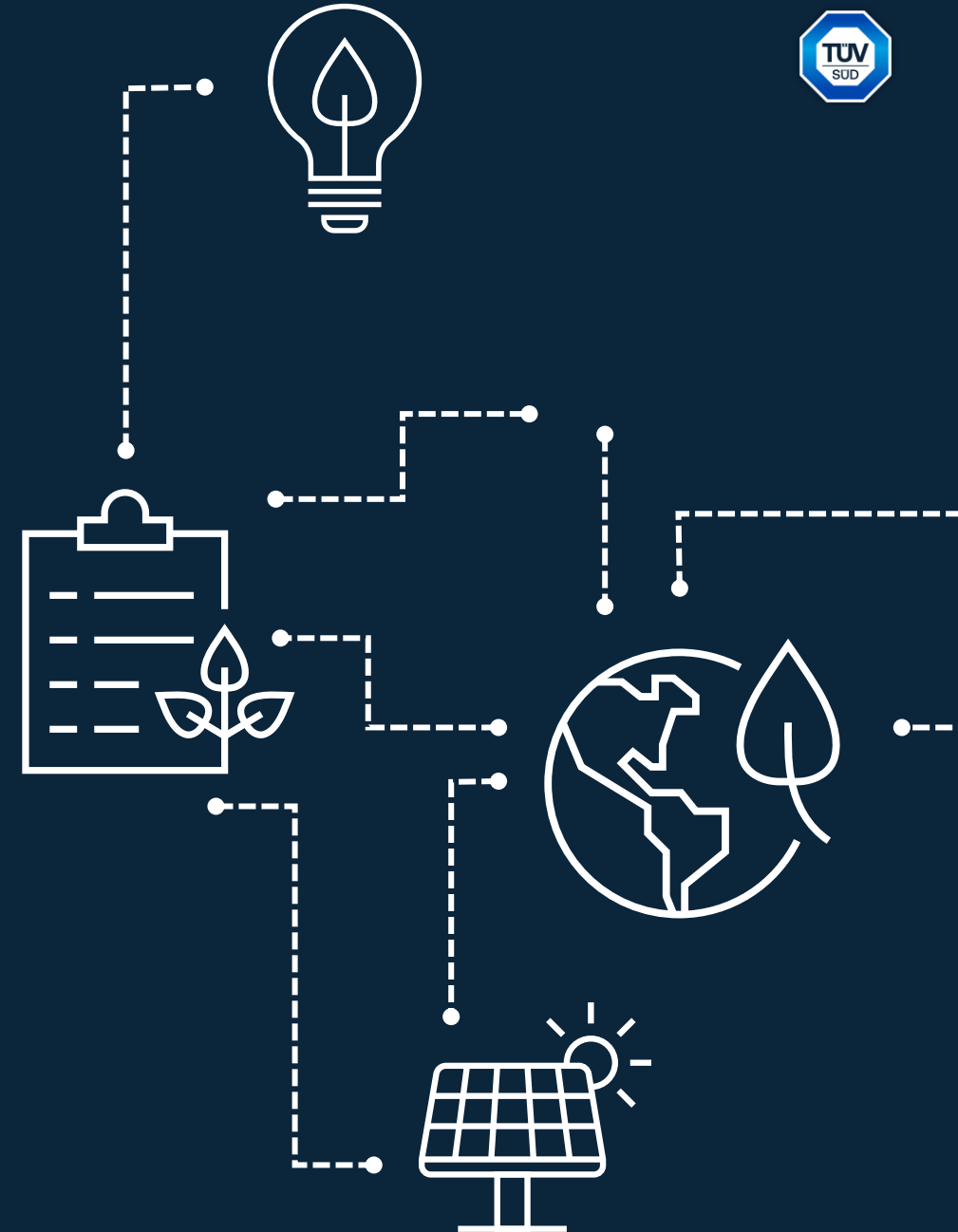
|  |                                                               |  |
|--|---------------------------------------------------------------|--|
|  | Project: CONSTRUCTION OF NEW PIPELINE FROM<br>GUEBIBA TO CFTP |  |
|  | HAZID/HAZOP/SIL TOR                                           |  |

**HAZID/HAZOP/SIL TOR**

**CONSTRUCTION OF NEW PIPELINE FROM GUEBIBA/TB TO CFTP**

# Estimating duration

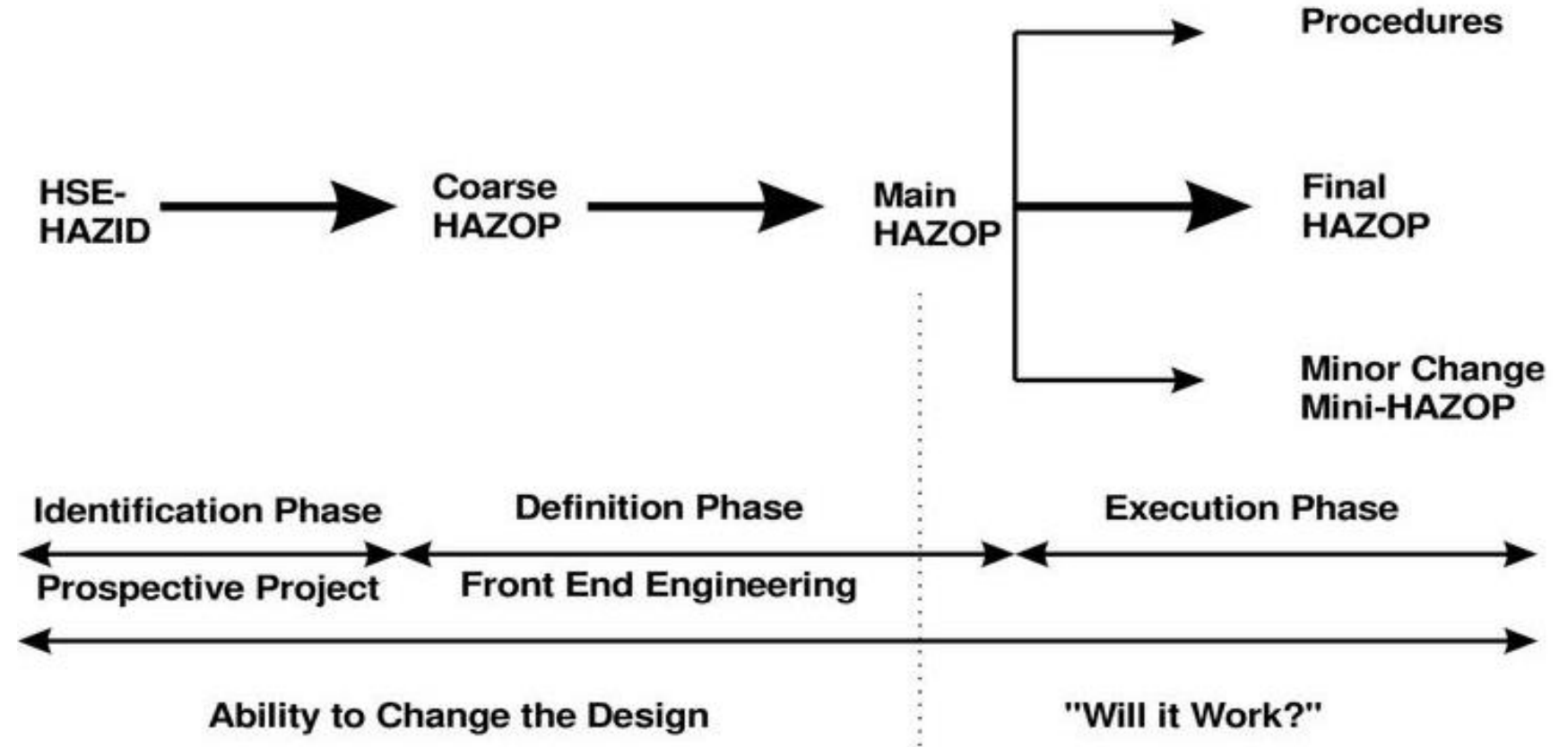
- Considerations when estimating duration
- Appropriate selection of guidewords
- Operating modes (in addition to 'normal' operation)
- Size of nodes
- Other factors
- Size of the team
- Experience of leader & members
- Study duration and team productivity



# HAZOP in Project Life Cycle

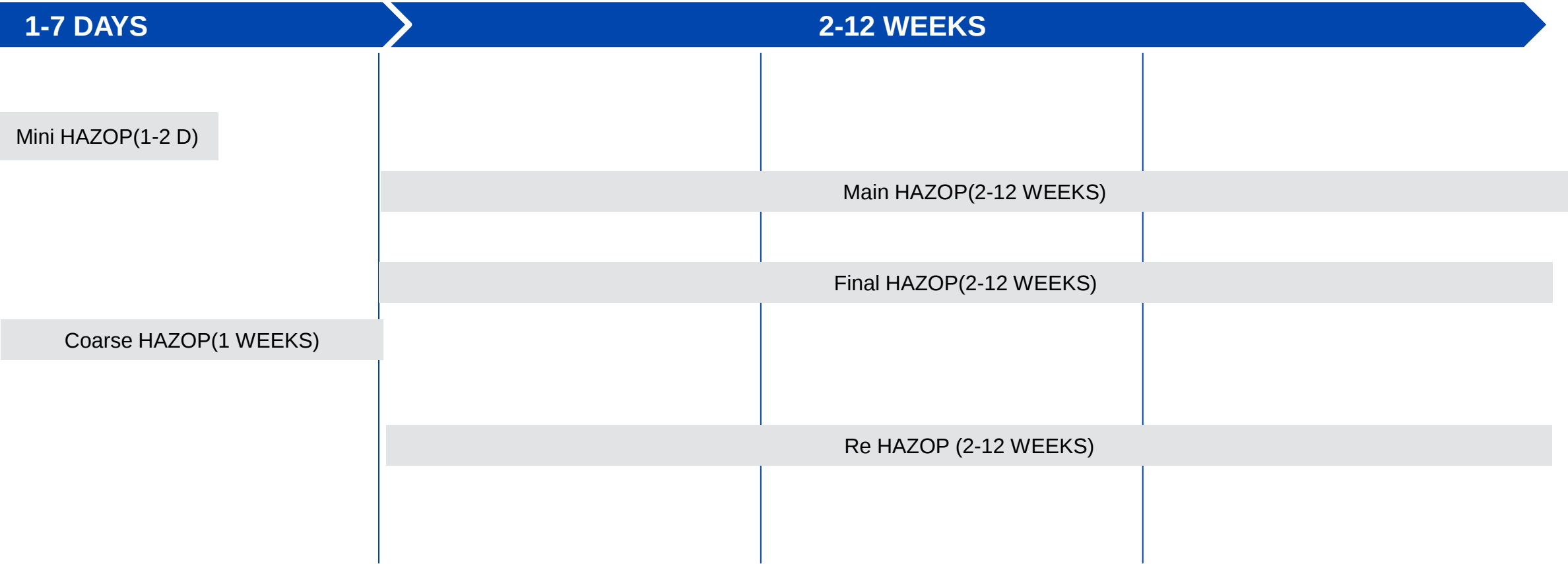


- Coarse HAZOP
- Main HAZOP
- Final HAZOP
- Mini HAZOP
- Re HAZOP
- 6-8 Hours / Day
- 4-8 Hours / P&ID
- 5 Days / week





# HAZOP in Project Life Cycle



# HAZOP dimension

- Number of process description pages (P Description)
- Number of Process Flow Diagrams (PFDs)
- Number of Piping & Instrumentation Diagrams (P&IDs)
- Number of pieces of Major Equipment (ME)
- Number of Nodes (Nd)
- Total time required to prepare and organize the study (TP)
- Total time required to execute the study (TS)
- Total time required to write the draft report (TW)



# Features of nodes selected

- Number of pieces of Major Equipment (ME)
- Number of Flow Control Valves (FCVs)
- Number of Level Control Valves (LCVs)
- Number of Pressure Control Valves (PCVs)
- Number of Temperature Control Valves (TCVs)
- Number of Pumps (Pumps)
- Number of Exchangers (Exchangers)





# Brainstorming sessions

- Time required to brainstorm a node
- Number of sessions where the node has been brainstormed (N)
- Number of expert members present in the session (Members)



# Time Required for HAZOP

- $TH = TP + TS + TW + C$
- TH: total time to perform the HAZOP study, in hours (h)
- TP: time to define, prepare and organize the study, in hours (h)
- TS: time to execute the study via brainstorming sessions, in hours (h)
- TW: time to write the first draft of the HAZOP report, in hours (h)
- C: Constant time related to preparation and Writing (30-70 h)
- 1 hour HAZOP presentation during the first day
- Review of First Node will take 6-8 Hours, it is essential to finalize it during the first Day
- First Node considered as 3 Nodes
- Starting from the Second Node , It will take 3 Hours for each node as average
- Small / simple: 2 hours
- Medium / moderate: 2 – 4 hours
- Large / complex: 4 – 6 hours (or more)





# Factors Related to Time Required for HAZOP

- Team size
- Level Of Experience
- Size of the process
- Complexity of the nodes and process
- Purpose, scope and objectives of the HAZOP study
- Team dynamics
- Fluency of team members in a common language
- Repeated Nodes or Streams
- Onsite or Offsite



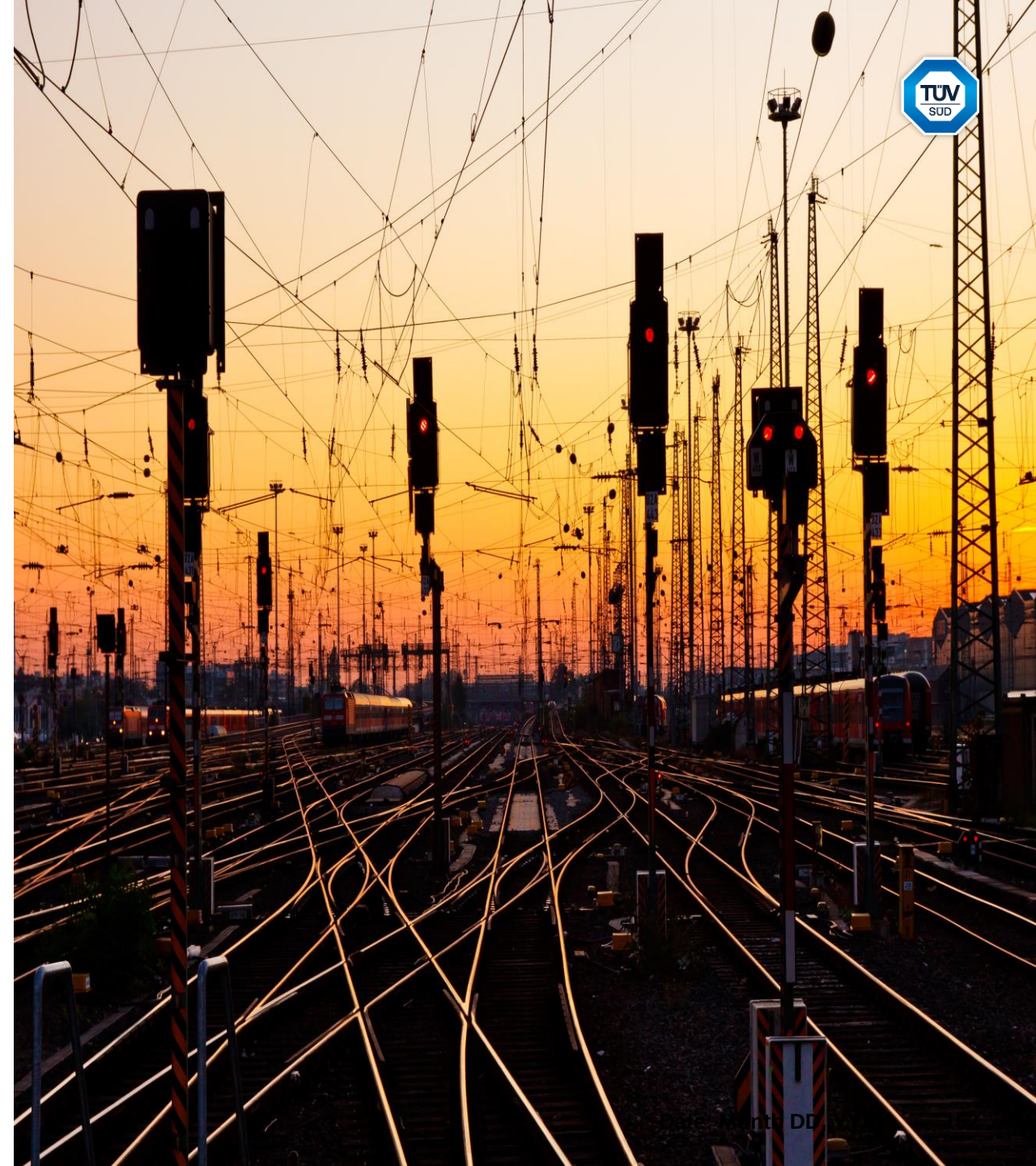


# Number Of Nodes

- Complex Package 8-10 Nodes per P&ID “Includes Different modes of operation “
- Simple Packages 1-4 Nodes Per P&ID
- Considering that each P&ID need approximately 1.5 Hour as Preparation
- Considering that each P&ID need approximately 1.5 Hour during Reporting
- Leader and secretary will spend 25% more time from than the team reviewing the team's comments on the draft minutes and updating the worksheets ( $0.25 * TS$ )
- Simple Node “line-by-line” /2H
- Super Nodes/4H-use combinations of lines and major vessels as nodes, to speed up studies. This approach provides a broader view of a process but it complicates the analysis and scenarios may be missed
- Global nodes/3H
- Complex nodes/6H

# Global nodes

- Global nodes allow initiating events that affect more than one node to be addressed
- Initiating events may affect the entire process or parts of it, for example, some external events such as flooding, or the global loss of utilities such as electric power. Thus, they may apply to multiple nodes or may not be specific to any particular node.
- Specific issues that arise in more than one node / system
- Examples include facility siting, human factors, and common piping issues.
- Need to look at hazards from the perspective of the overall process
- HAZOP study practitioners must avoid omitting scenarios that may not be identified by focusing on individual nodes. For example, multiple failure scenarios may involve causes originating from more than one node or system.





# Human Error as a Cause In HAZOP?

Many team members will instantly object when human error is recorded as a cause in a HAZOP workshop. Their point of view is that operators are highly trained personnel and they will not inadvertently open or close a valve. Comment: It is true that operating personnel are trained and they are not expected to make errors but stress, upset conditions at plant, start-up mode or equipment where frequent change-overs are required can lead to operator making mistake. So, generally the human error as a cause is accepted and used in HAZOP studies.





# Operating Procedure as a Safeguard In HAZOP?



Operating procedure is a first safeguard that comes to mind of most team members when they are struggling to identify safeguards for an accident scenario. I personally resist accepting it as a safeguard and force the team members to do more thinking and propose automatic safeguard rather than a simple operating procedure. Operating procedure as a safeguard is applicable almost in all scenarios and the HAZOP worksheets will fill up quite quickly if we start writing operating procedure as a safeguard. Having said that there are situations where it is not practical to engineer an automatic safeguard, therefore, only on those situations operating procedure can be taken as a safeguard.



# Non-return valve as a Safeguard In HAZOP?

- A check valve is not a tight shut-off device and there can be a certain leakage through it when it is in closed position especially if it is not inspected and maintained on periodic basis. Sometimes, it is recommended that two dissimilar type check valves are installed in series to minimize the reverse flow but only in situations where reverse flow can cause contamination issues rather than over-pressurization and integrity threat.
- If the purpose of the check valve is to protect the low pressure rated system from the high pressure rated system then check valves may not be very helpful. The preferred solution for such situations is to install an automatic shutdown valve on the line which should close on detection of reverse flow or high pressure at the low pressure rated system. Some designers measure differential pressure across the control valve assembly on the line to detect reverse flow and close automatic shutdown valve to protect low pressure rated system.



# Passing of Pressure Safety Valve as a Cause In HAZOP?

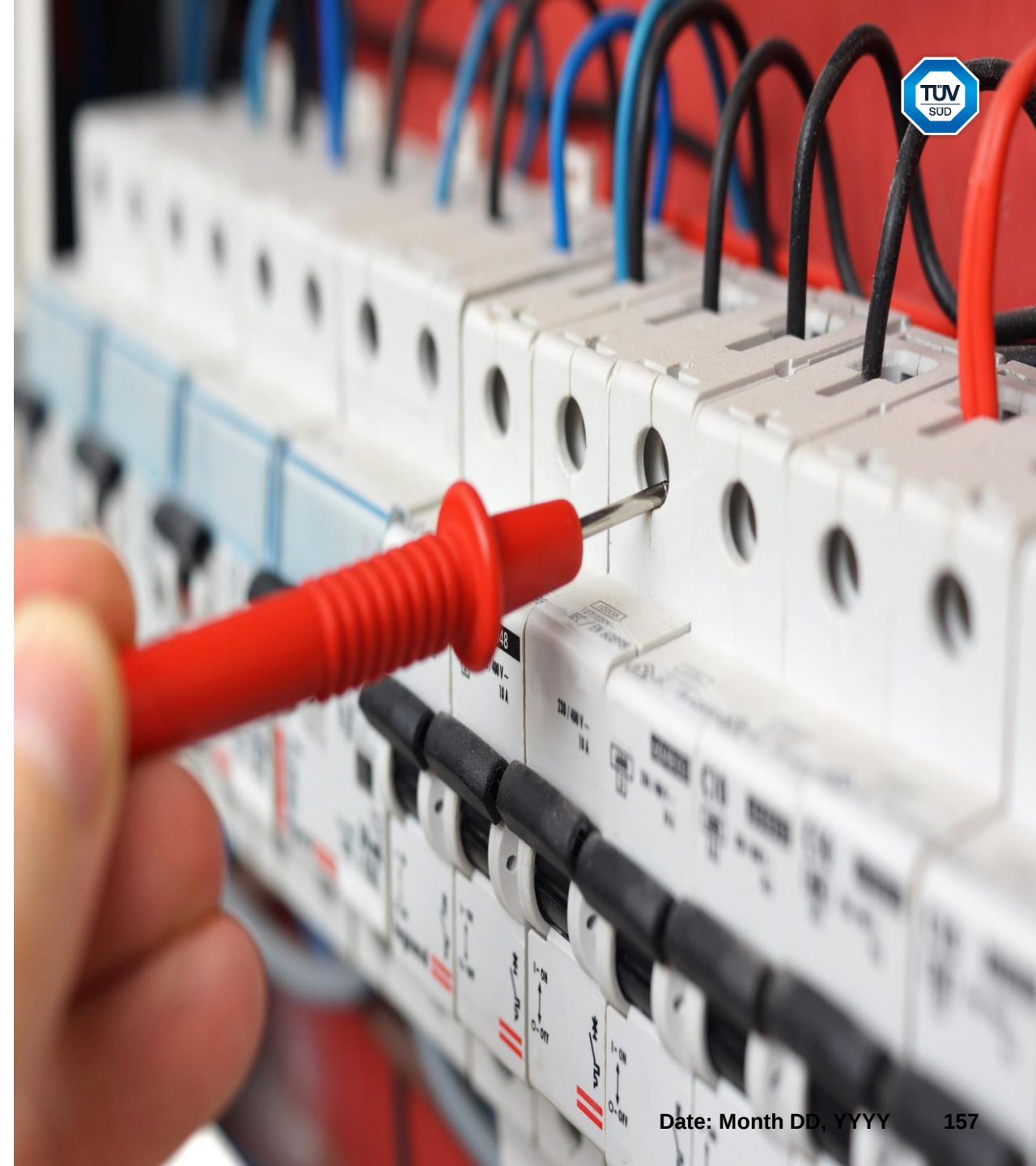
It is true that a PSV can pass and there could be a leakage through it causing a reduced flow through the line. However, there are certain safeguards which are considered as our last layer of defense before an accident happens. These are pressure safety valves, blowdown valves, safety instrumented system and a few more. Generally, in a HAZOP study we do not fail our last layer of defense to build a scenario. Therefore, failed condition of pressure safety valve, blowdown valve and safety instrumented system are generally not taken as a cause for building HAZOP scenarios.





# Control Loop failure as a Cause In HAZOP?

The control loops are usually connected with plant's Distributed Control System (DCS). They normally control level, flow, pressure, temperature etc. In its simplest form, they consist of an initiator (e.g. transmitter, analyser), a logic solver (e.g. PLC) and a final control element (e.g. control valve, trip relay). There could be multiple initiators or final control elements depending upon the design. Failure of a control loop is a valid HAZOP cause but there is a confusion about how it failed, for example, partially or completely. Some team members argue that we should not take failure of both transmitter and control valve at the same time. It's a double jeopardy. To be on a safe side, when control loop failure is taken as a cause in a HAZOP study it is taken as a complete failure of the loop and we assume that the loop is dead and none of its components is still live or operational



# Alarms as a Safeguard In HAZOP?

- When a process deviation occurs then process control is the first layer which comes into action and try to control the process variable e.g. pressure, temperature, level or flow within the defined limits. However, the process control may not work on all occasions and the process variable can go out of the limits. The second layer of protection is generally the alarm which will get the operator's attention for manual action so that process variable can be controlled with the limits. Before taking the credit of an alarm in a HAZOP study several factors should be considered.
- How much time is available for the operator to take action and bring the process variable within the limits before the next layer of protection kicks in or a dangerous situation arises which can lead to an accident. So, the time available to the operator for completion of his action is an important consideration before taking credit for an alarm.
- The other factors are requirement of written instructions for operator action, training of the operators and registration of the alarms for periodic maintenance before alarm credit can be claimed.
- There is a tendency to propose new alarms in a HAZOP study by the team. The flood of alarms during emergency is not helpful for the operator to quickly diagnose the situation and take appropriate action.



# Points to be considered In HAZOP?

- Power outage?
- Simultaneous operation of more than required pumps/compressors ?
- Should we HAZOP Fire Water System in the same way as we do HAZOP for Process Units?
- Should we do risk ranking in the HAZOP meeting so that we can prioritize the implementation of the recommendations?

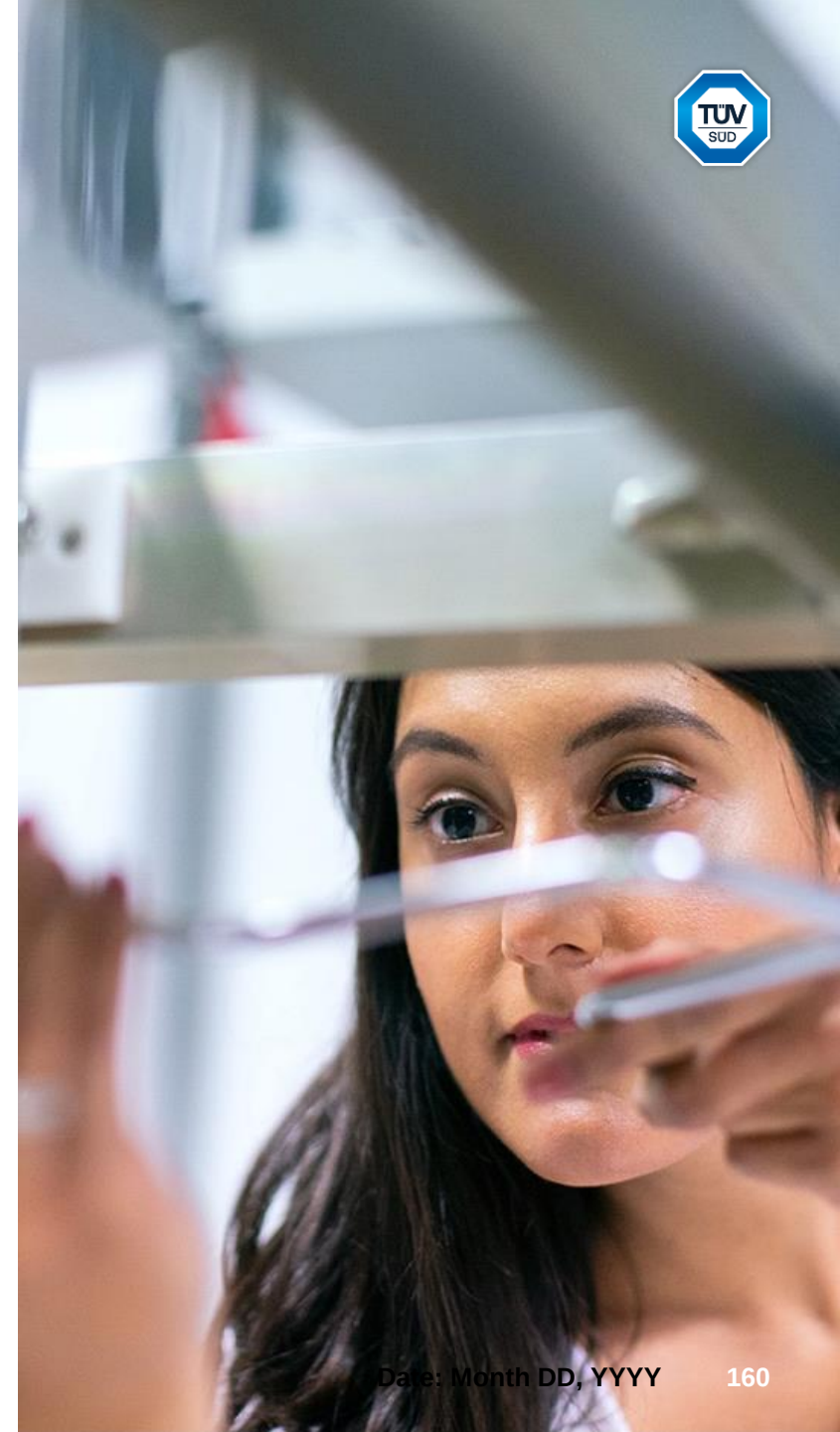




# Summary

What we have learned in the module

- What is the REHAZOP ?
- What is the LOPA ?
- What is HAZOP/LOPA?
- Time Required for HAZOP



# Exercise 4 - Questions



Q1) Where LOPA may not be appropriate ?

- A. Low severity events
- B. Domino events
- C. Integrity management issues
- D. Design errors
- E. Events initiated by external factors
- F. All of the above

# Exercise 4 - Questions



Q2) The requirement was for LOPA to be carried before completion of the HAZOP studies.

- A. True
- B. False
- C. Sometimes Depend on the process scope itself



# Exercise 4 - Questions



Q3) What is the HAZOP?

Q4) WHO is Required in HAZOP study?

Q5) What are the key documents and information required during HAZOP?

Q6) What are the Key Points to be considered during ReHAZOPs ?

# Note



# Any Question?



**Follow us on:**



[tuvsud.com](https://tuvsud.com)  
[info@tuvsud.com](mailto:info@tuvsud.com)



# CERTIFIED PHA - HAZOP LEADER

## Checklists



01

**Module 1**  
INTRODUCTION

02

**Module 2**  
PROCESS SAFETY MANAGEMENT

03

**Module 3**  
HAZOP

04

**Module 4**  
REHAZOP & LOPA

05

**Module 5**  
Checklists

06

**Module 6**  
WHAT IF & FMEA

07

**Module 7**  
LEADERSHIP

08

**Module 8**  
BOWTIE ANALYSIS

# 5 Checklists

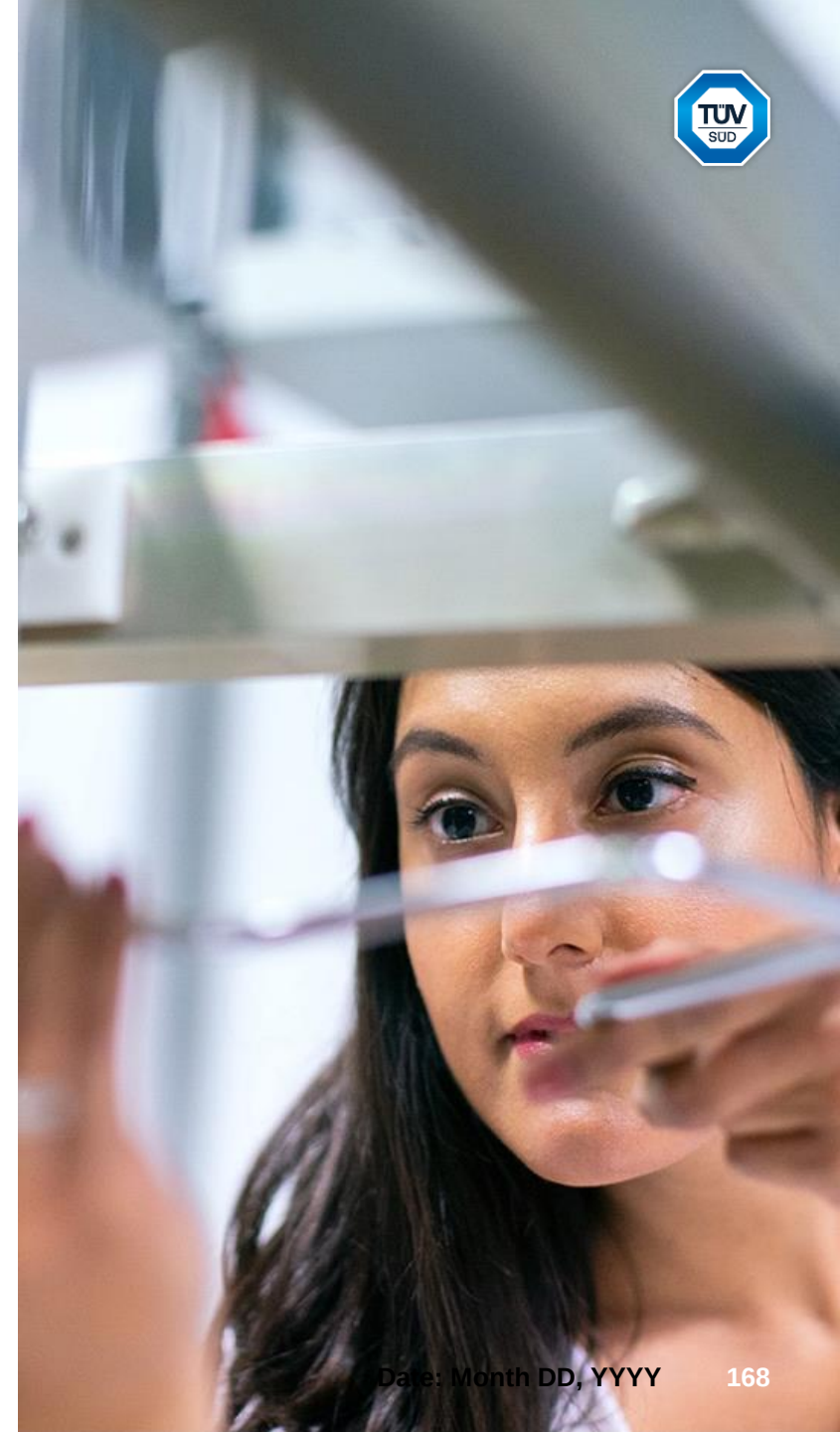


# Module 5

## Checklists

In this module

- Definition Of Checklists
- Objectives of Checklists
- Checklists steps





# Checklists



- By definition a checklist is an aide memoire, for example the 'pre-take-off checks' carried out by a pilot of an aircraft. It uses carefully compiled comprehensive list of protective measures, procedural steps, material properties, hazards or 'good practice' design features that have been compiled by experienced personnel for a particular application
- Checklist Analysis can be used at any time throughout a design or with an existing facility. Where there is a lack of experienced personnel the use of existing checklists is a valuable tool for identifying hazards. Useful where teams of personnel are not available and individuals are required to perform the analysis.

| Checklist For Assessment of Different Type of Risks - (Sample Checklist) |                                                                                                   |                                       |           |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------|-----------|
| (A) Product Size Risks                                                   |                                                                                                   |                                       |           |
| Following generic risks are associated with the product size             |                                                                                                   |                                       |           |
| Sr.                                                                      | Check Point / Defect Statement                                                                    | Check Mark (✓) the Appropriate Column |           |
|                                                                          |                                                                                                   | Yes                                   | No or N/A |
| 1)                                                                       | Estimated size of the product in LOC or FP?                                                       |                                       |           |
| 2)                                                                       | Degree of confidence in estimated size estimate?                                                  |                                       |           |
| 3)                                                                       | Estimated size of product in number of programs, files, transactions?                             |                                       |           |
| 4)                                                                       | Percentage deviation in size of product from average for previous products?                       |                                       |           |
| 5)                                                                       | Size of database created or used by the product?                                                  |                                       |           |
| 6)                                                                       | Number of users of the product?                                                                   |                                       |           |
| 7)                                                                       | Number of projected changes to the requirements for the product? Before delivery? after delivery? |                                       |           |
| 8)                                                                       | Amount of reused software?                                                                        |                                       |           |

# Checklists

- Checklist Analysis is an experience-based methodology and its value is dependent on the quality of the checklist.
- Operating systems are defined and lists of questions are generated about standard design and operating practices for each system.
- Checklist questions need to be developed by a multidisciplinary team with experience in the process being studied.
- Checklists are best tailored specifically for an individual company or plant and built upon over time.
- Questions usually require “Yes”, “No” or “Requires more information” answers.
- Can be used at any time in the facility lifecycle to evaluate materials, equipment and procedures, but is especially effective combined with a pre-start-up safety review if a previous hazards analysis has been conducted at the detailed design stage.
- Can be as detailed as required for the purpose.
- Can be combined with What-If Analysis for comprehensive evaluation of hazards.
- Can be used as an investigative tool to identify hazards and an audit tool to verify designs and installations.
- Is not an aid to identification of unknown hazards.
- Does not identify operability problems well.

# Objectives of Checklist Analysis



- to verify compliance with design, codes and regulations at start-up.
- to help control management of change.
- to aid in a comparative review of process not yet built.
- to act as an aid in training people inexperienced in a process.
- Checklists generated from experience, standards and codes and industry guidelines and any other authoritative references such as engineering and construction drawings, equipment specifications and previous hazards analysis study findings.
- Checklists can be developed by a number of people with experience in specific parts of the process or plant.





# Steps in Checklist Analysis



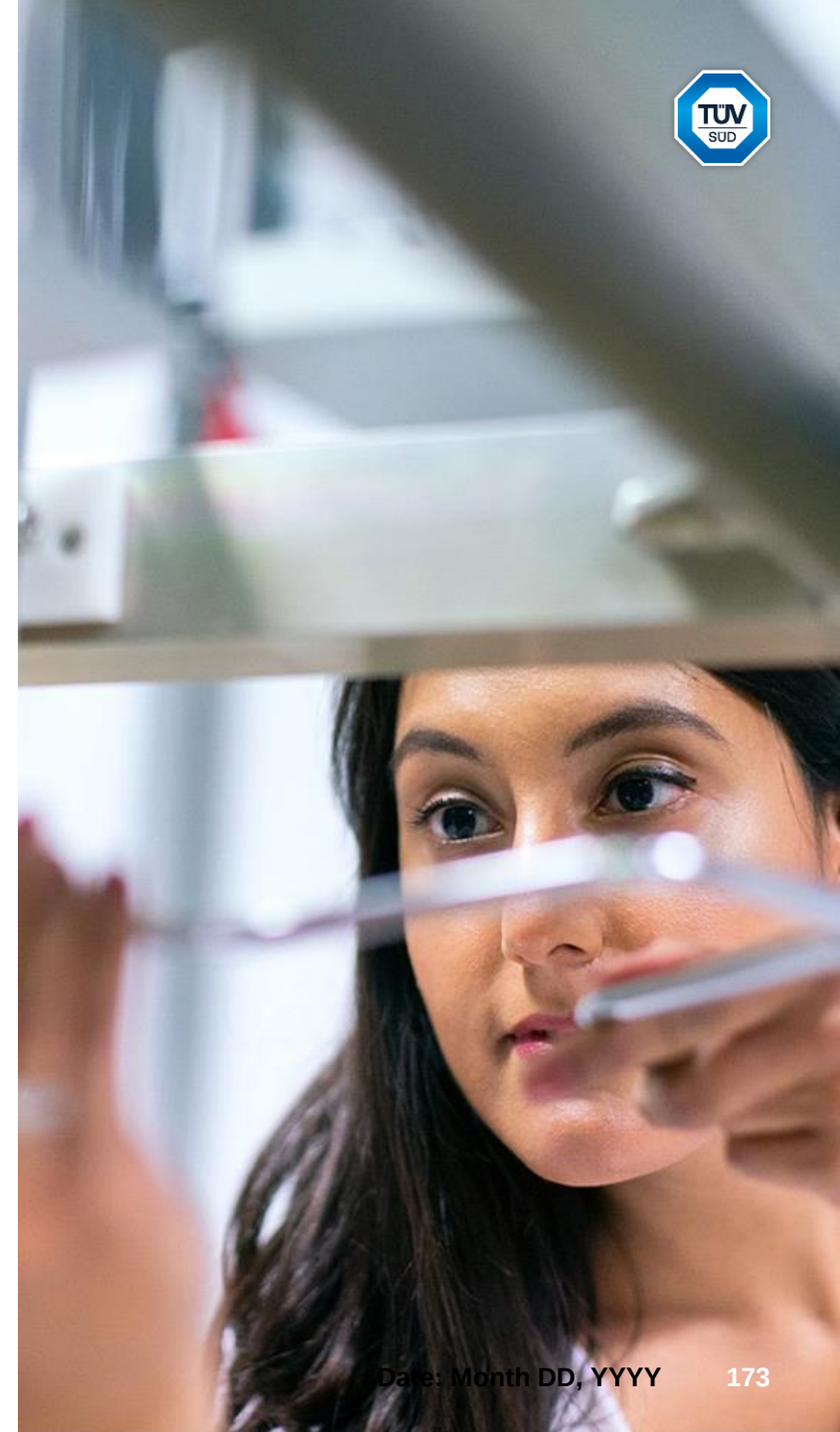
- Acquire or develop appropriate checklists.
- Expert team members tour the subject process with leader and compare equipment and operation to checklist items.
- Deficiencies are noted.



# Summary

What we have learned in the module

- Definition Of Checklists
- Objectives of Checklists
- Checklists steps



# Exercise 5 - Questions



Q1) What are the Steps in Checklist Analysis ?

Q2) What are the Objectives of Checklist Analysis ?



# Note



# Any Question?



**Follow us on:**



[tuvsud.com](https://tuvsud.com)  
[info@tuvsud.com](mailto:info@tuvsud.com)

# CERTIFIED PHA - HAZOP LEADER

## WHAT IF & FMEA



01

**Module 1**  
INTRODUCTION

02

**Module 2**  
PROCESS SAFETY MANAGEMENT

03

**Module 3**  
HAZOP

04

**Module 4**  
REHAZOP & LOPA

05

**Module 5**  
Checklists

06

**Module 6**  
WHAT IF & FMEA

07

**Module 7**  
LEADERSHIP

08

**Module 8**  
BOWTIE ANALYSIS



# 6

## WHAT IF & FMEA

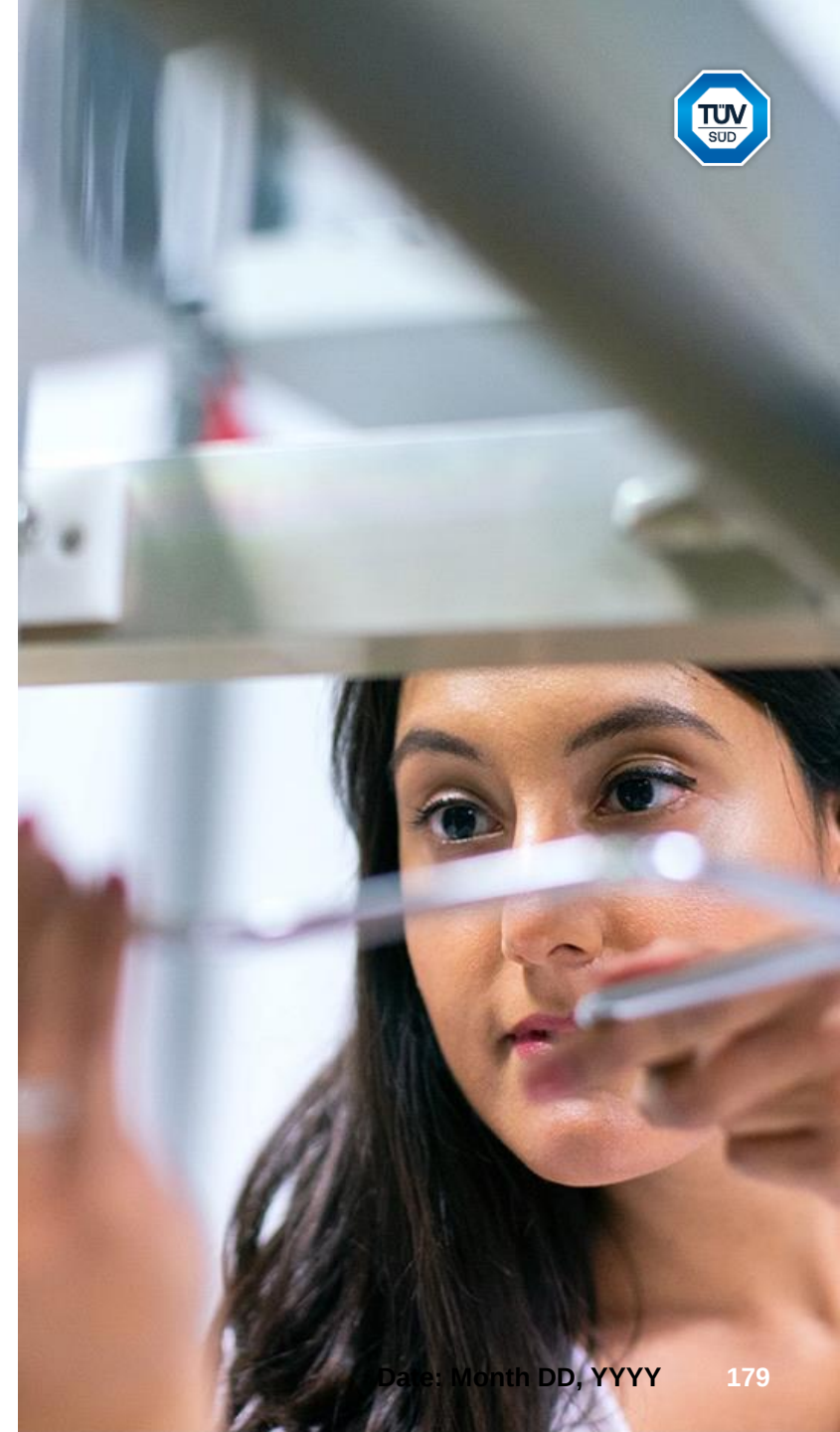


# Module 6

## WHAT IF & FMEA

In this module

- What If Analysis
- What If Analysis STEPS
- FMEA
- Steps in an FMEA
- Limitations of PHA



# What If Analysis



- What If can be used at any time for new or existing facilities. Requires an experienced team and adequate preparation. Best results when used in conjunction with the Checklist method otherwise the team's imagination may prove inadequate at the time of analysis.
- What-If Analysis uses a creative team brainstorming “what if” questioning approach to the examination of a process or operation to identify potential hazards and their consequences. Users should be experienced and creative thinkers. Questions that begin with “what-if” are formulated by engineering personnel experienced in the process or operation and subdivided into specific categories of interest.

| Scope:<br>Status |              |            | What If Analysis |
|------------------|--------------|------------|------------------|
| What If          | Consequences | Safeguards | Recommendations  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |
|                  |              |            |                  |



# What If Analysis

- Experienced personnel brainstorming a series of questions that begin, "What if...?"
- Each question represents a potential failure in the facility or mis-operation of the facility
- The response of the process and/or operators is evaluated to determine if a potential hazard can occur
- If so, the adequacy of existing safeguards is weighed against the probability and severity of the scenario to determine whether modifications to the system should be recommended
- "What if the raw material being introduced is the wrong concentration?"
- "What if the operator forgot to manually close the valve?"
- Questions can also focus on specific consequences such as process safety, operating procedures, human error or environmental safety. Does not easily generate operability information.
- Questions are applied to existing P&IDs and process descriptions.
- Questions are usually added as the analysis progresses.

# What If Analysis



- Hazards are identified, existing safeguards noted and qualitative severity and likelihood ratings are assigned to aid in risk management decision-making.
- Loose structure necessitates experienced team.
- Can only provide high level of assurance with very knowledgeable, experienced and creative team.
- Often used at design concept stage and to analyse proposed changes to a facility.

| Severity \ Likelihood     | Minimal<br>5 | Minor<br>4 | Major<br>3 | Hazardous<br>2 | Catastrophic<br>1 |
|---------------------------|--------------|------------|------------|----------------|-------------------|
| Frequent<br>A             |              |            |            |                |                   |
| Probable<br>B             |              |            |            |                |                   |
| Remote<br>C               |              |            |            |                |                   |
| Extremely Remote<br>D     |              |            |            |                |                   |
| Extremely Improbable<br>E |              |            |            |                | *                 |

|             |
|-------------|
| High Risk   |
| Medium Risk |
| Low Risk    |

\* Unacceptable with Single Point and/or Common Cause Failures

# What-If –Steps

- 1. Provide relevant information to selected team members in sufficient time before the study for their input in developing “What if” questions.
- 2. Leader divides process into logical systems and subsystems.
- 3. Scope and objectives of study are explained.
- 4. Existing safety precautions and equipment are described.
- 5. Team reviews information to generate more questions related to the systems of the process.
- 6. List of questions is made.
- 7. Systems and subsystems are analysed from the beginning of the process to the end by applying the relevant “what if” questions.
- 8. Potential hazards are identified and consequences estimated and documented.
- 9. Severity and likelihood factors are given and a risk ranking assigned and documented.
- 10. Recommendations for improvement are made and documented.





# What-If Question Areas

- Equipment failures
  - What if ... a valve leaks?
- Human error
  - What if ... operator fails to restart pump?
- External events
  - What if ... a very hard freeze persists?



# What-If/Checklist Analysis

## What-If +Checklist

- What-if/Checklist Analysis combines the creative brainstorming features of the What-If Analysis with the systematic features of the Checklist Analysis to provide a comprehensive method of identifying hazards.
- Creative questioning augments the systematic experienced based checklist to provide a more complete study.
- Checklists are generally structured to focus on general sources of hazards and accidents.
- Study can begin with a checklist to which “what-if” questions are applied to round out gaps in the list.
- Alternatively, study can begin with a brainstormed identification of hazards followed by the structure of a checklist.
- Can be used successfully at any stage in facility lifecycle.
- Requires a team experienced in the process under review.
- Usually provides a less detailed review than the more structured analyses such as HAZOP.
- Can be structured to provide detailed analysis but this can be time consuming unless checklists and questions can be used from previous studies.

# Objectives of What-If /Checklist Analysis

- to identify and evaluate the most common hazards in a process.
- to provide a qualitative evaluation of the consequences of accident outcomes.
- to evaluate the adequacy of existing safeguards.





# Failure Mode and Effects Analysis (FMEA)



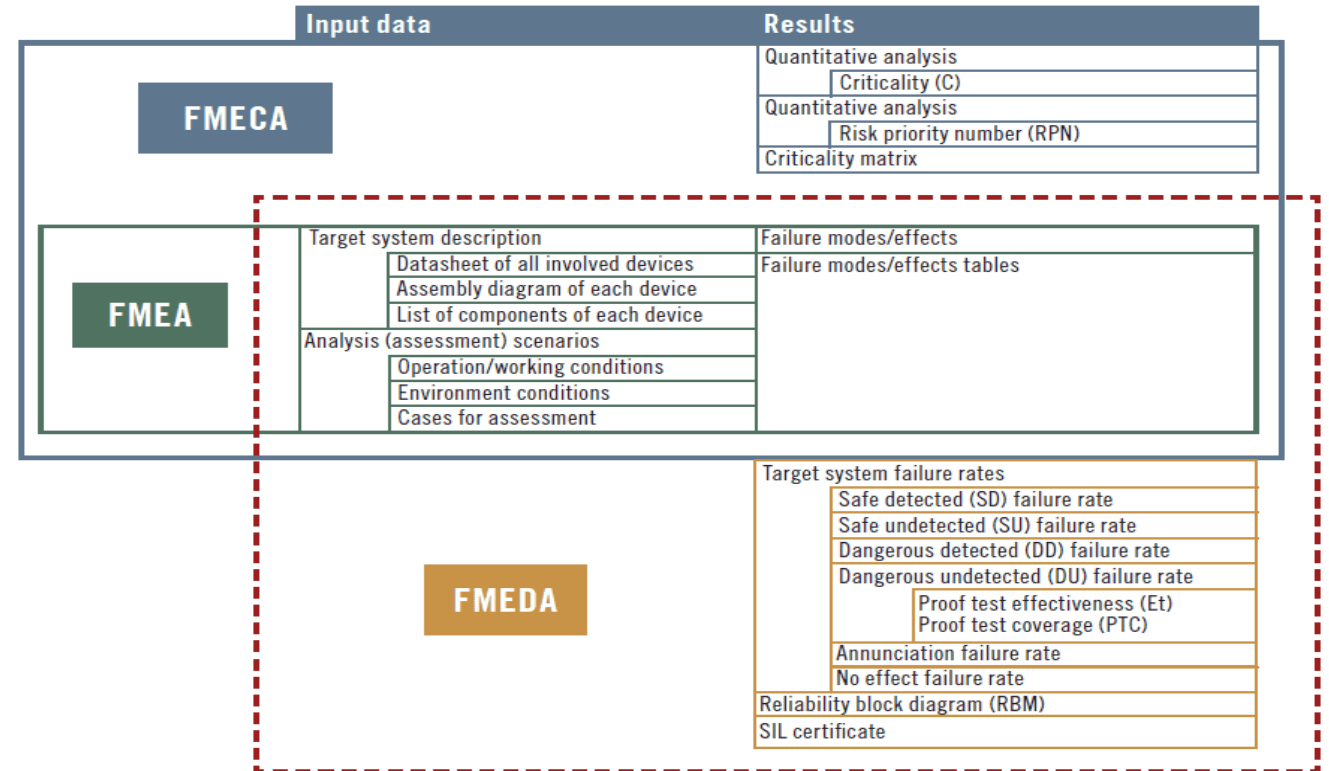
- Analysing specific systems or items of equipment that are best handled as objects rather than by the use of parameters or operations.
- Analysing pumps, compressors and items of equipment having interactive mechanical and/or electrical components.
- Splitting equipment into components and further splitting into sub-components
- Postulating failures, examine effects, record safeguards, and recommend modifications
- A FMEA considers in a systematic and rigorous manner all of the possible single failure modes of the individual plant items and elements in a system. The effects of each failure on the item itself and on the rest of the system are identified and recorded..
- The analysis is usually carried out by a small team who should have detailed knowledge of the equipment. In a FMECA the criticality of the consequences and likely frequency are also assessed and recorded.

|             |  |                                   |  |               |  |               |  |               |  |
|-------------|--|-----------------------------------|--|---------------|--|---------------|--|---------------|--|
| System      |  | Design Verification Process       |  | Potential     |  | FMEA Number   |  | Project III   |  |
| Subsystem   |  | Failure Mode and Effects Analysis |  |               |  | Prepared By   |  | Houston Mayer |  |
| Component   |  |                                   |  | (Design FMEA) |  | FMEA Date     |  | 22/1          |  |
| Design Lead |  | Houston Mayer                     |  | Key Date      |  | Revision Date |  | 21/E          |  |
| Core Team   |  | See Project III R1 Report         |  |               |  | Page          |  | 1 of 6        |  |

| Item / Function                                                               | Potential Failure Mode(s)                                                                                                                                                                                                  | Potential Effect(s) of Failure                                                                   | C | S | Potential Cause(s)/ Mechanism(s) of Failure | D | P | Current Design Controls                                                                        | C | RPN | Recommended Action(s)                                                                                                                                              | Responsibility & Target Completion Date | Action Results                                                                       |     |     |     |         |
|-------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|---|---|---------------------------------------------|---|---|------------------------------------------------------------------------------------------------|---|-----|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------|--------------------------------------------------------------------------------------|-----|-----|-----|---------|
|                                                                               |                                                                                                                                                                                                                            |                                                                                                  |   |   |                                             |   |   |                                                                                                |   |     |                                                                                                                                                                    |                                         | Actions Taken                                                                        | NEW | NEW | NEW | New RPN |
| Customer sends in a quote request for product.                                | System, Software, Integration and Shipping requirements overlooked by customer.                                                                                                                                            | Customer needs not fully met by delivered system.                                                | 7 |   | Human error                                 | 1 |   | Design configuration tool.                                                                     | 3 | 21  | Use configuration tool when available.                                                                                                                             | Closed 10/21/99                         |                                                                                      |     |     |     | 0       |
| Requirement entered and verified by Inside Sales in config. tool.             | Data entry error                                                                                                                                                                                                           | System compatibility requirements not evaluated by config. tool.                                 | 3 |   | Human error                                 | 1 |   | Order verified by a configuration tool.                                                        | 3 | 9   | Continue order verification by configuration tool.                                                                                                                 | Closed 10/21/99                         |                                                                                      |     |     |     | 0       |
| Sales identifies need for CD or SHC                                           | Specific packing, labeling and shipping requirements may not be fully addressed.                                                                                                                                           | On time delivery and integrity of the product may be compromised if this issue is not addressed. | 7 |   | Requirements Overlooked.                    | 5 |   | Customer Inspection Instruction/ Special Handling Codes Process 013-001-02                     | 3 | 63  | Pedish comprehensive procedure for the 1st Article Process.                                                                                                        | Jan-00                                  | Customer shipping requirements reviewed by quality assurance in 1st Article process. |     |     |     | 0       |
|                                                                               | Position of the DHR in DCD label packet not identified by GE. Requirement in Purchase Specification for monopod, but not identified on Bill of Material. DCD Card content requirements not identified in Build Procedures. | Loss of business with the customer.                                                              | 1 |   | Requirements Overlooked.                    | 5 |   | CD 013-001-006                                                                                 | 1 | 5   | Revisit contents of GE CD 013-001-006 to assure all requirements are clearly communicated to the warehouse operators and quality technicians using these documents | Sep-00                                  | OPEN 8/21/00                                                                         |     |     |     |         |
| QA and Pack and Ship Team reviews customer requirements during a 1st Article. | Specific packing, labeling and shipping requirements may not be fully addressed.                                                                                                                                           | Customer's full expectations may not be realized.                                                | 7 |   | Requirements overlooked.                    | 3 |   | Customer requirements physically verified by quality assurance during the 1st Article process. | 3 | 63  | Continue current process.                                                                                                                                          | Closed 10/25/99                         |                                                                                      |     |     |     | 0       |
| Inside sales submits                                                          | Data entry error                                                                                                                                                                                                           | Order Processing                                                                                 | 1 |   | Human Error                                 | 1 |   | Customer requirements                                                                          | 3 | 3   | Continue current                                                                                                                                                   | Closed 1/25/00                          |                                                                                      |     |     |     | 0       |

# Failure Mode and Effects Analysis (FMEA)

FMEA is not strictly speaking a hazard identification technique, but it provides an important source of hazard information because it documents and describes all the ways in which individual pieces of equipment can fail and the effects of such failure on a facility



# Failure Mode and Effects Analysis (FMEA)

- Can be used at all stages of a facility's life and can be easily updated for plant modifications.
- Requires knowledge of equipment function and failure modes as well as facility function and its potential response to equipment failure.
- Requires consistent format and procedure to help ensure efficient study.
- Can be conducted at component or system level.
- Each equipment item within a defined system is evaluated for its failure modes.
- Identifies and describes all possible ways in which equipment fails (failure modes) e.g. On/off, open/closed, etc.
- Identifies only single failure modes that cause or contribute to an accident (e.g. individual failure is considered an independent occurrence).
- Not effective in identifying the combinations of equipment failures that result in an accident.
- System level hazards can be analyzed by focusing on the individual pieces of equipment that make up the system while keeping in mind the overall effect on the subject system.



# FMEA Methodology



- **Define the Scope/Function:**
- Identify the process, product, or system to be analysed.
- Assemble a cross-functional team with relevant expertise.

| Function                                      | Potential Failure Mode          | Potential Effects(s) of Failure          | S | Potential Cause(s) of Failure         | O | Current Process Controls                 | D  | R   | P  | C | Recommendation Action(s) |
|-----------------------------------------------|---------------------------------|------------------------------------------|---|---------------------------------------|---|------------------------------------------|----|-----|----|---|--------------------------|
| Dispense amount of cash requested by customer | Does not dispense cash          | Customer very dissatisfied               | 8 | Out of cash                           | 5 | Internal low-cash alert                  | 5  | 200 | 45 |   |                          |
|                                               |                                 | Incorrect entry to demand deposit system |   | Machine jams                          | 3 | Internal jam alert                       | 10 | 240 | 24 |   |                          |
|                                               |                                 | Discrepancy in cash balancing            |   | Power failure during transaction      | 2 | None                                     | 10 | 160 | 16 |   |                          |
|                                               | Dispenses too much cash         | Bank loses money                         | 6 | Bills stuck together                  | 2 | Loading procedure (riffle ends of stack) | 7  | 84  | 12 |   |                          |
|                                               |                                 | Discrepancy in cash balancing            |   | Denominations in wrong trays          | 3 | Two-person visual verification           | 4  | 72  | 18 |   |                          |
|                                               | Takes too long to dispense cash | Customer somewhat annoyed                | 3 | Heavy computer network traffic        | 7 | None                                     | 10 | 210 | 21 |   |                          |
|                                               |                                 |                                          |   | Power interruption during transaction | 2 | None                                     | 10 | 60  | 6  |   |                          |
|                                               |                                 |                                          |   |                                       |   |                                          |    |     |    |   |                          |

# FMEA Methodology

- **Identify Failure Modes:**
- List all the ways a component, process, or system could fail.
- Consider potential failures from various perspectives, including design, manufacturing, and user operation.

| Function                                      | Potential Failure Mode          | Potential Effects(s) of Failure          | S | Potential Cause(s) of Failure         | O | Current Process Controls                 | D  | R<br>P<br>N | C<br>R<br>I<br>T | Recommended Action(s) |
|-----------------------------------------------|---------------------------------|------------------------------------------|---|---------------------------------------|---|------------------------------------------|----|-------------|------------------|-----------------------|
| Dispense amount of cash requested by customer | Does not dispense cash          | Customer very dissatisfied               | 8 | Out of cash                           | 5 | Internal low-cash alert                  | 5  | 200         | 45               |                       |
|                                               |                                 | Incorrect entry to demand deposit system |   | Machine jams                          | 3 | Internal jam alert                       | 10 | 240         | 24               |                       |
|                                               |                                 | Discrepancy in cash balancing            |   | Power failure during transaction      | 2 | None                                     | 10 | 160         | 16               |                       |
|                                               | Dispenses too much cash         | Bank loses money                         | 6 | Bills stuck together                  | 2 | Loading procedure (riffle ends of stack) | 7  | 84          | 12               |                       |
|                                               |                                 | Discrepancy in cash balancing            |   | Denominations in wrong trays          | 3 | Two-person visual verification           | 4  | 72          | 18               |                       |
|                                               | Takes too long to dispense cash | Customer somewhat annoyed                | 3 | Heavy computer network traffic        | 7 | None                                     | 10 | 210         | 21               |                       |
|                                               |                                 |                                          |   | Power interruption during transaction | 2 | None                                     | 10 | 60          | 6                |                       |
|                                               |                                 |                                          |   |                                       |   |                                          |    |             |                  |                       |

# FMEA Methodology

- **Determine Effects of Each Failure Mode:**
- Assess the consequences of each identified failure mode on the system and its stakeholders.
- Evaluate how it impacts performance, safety, and customer satisfaction.

| Function                                      | Potential Failure Mode          | Potential Effects(s) of Failure          | S | Potential Cause(s) of Failure         | O | Current Process Controls                 | D  | R<br>P<br>N | C<br>R<br>I<br>T | Recommended Action(s) |
|-----------------------------------------------|---------------------------------|------------------------------------------|---|---------------------------------------|---|------------------------------------------|----|-------------|------------------|-----------------------|
| Dispense amount of cash requested by customer | Does not dispense cash          | Customer very dissatisfied               | 8 | Out of cash                           | 5 | Internal low-cash alert                  | 5  | 200         | 45               |                       |
|                                               |                                 | Incorrect entry to demand deposit system |   | Machine jams                          | 3 | Internal jam alert                       | 10 | 240         | 24               |                       |
|                                               |                                 | Discrepancy in cash balancing            |   | Power failure during transaction      | 2 | None                                     | 10 | 160         | 16               |                       |
|                                               | Dispenses too much cash         | Bank loses money                         | 6 | Bills stuck together                  | 2 | Loading procedure (riffle ends of stack) | 7  | 84          | 12               |                       |
|                                               |                                 | Discrepancy in cash balancing            |   | Denominations in wrong trays          | 3 | Two-person visual verification           | 4  | 72          | 18               |                       |
|                                               | Takes too long to dispense cash | Customer somewhat annoyed                | 3 | Heavy computer network traffic        | 7 | None                                     | 10 | 210         | 21               |                       |
|                                               |                                 |                                          |   | Power interruption during transaction | 2 | None                                     | 10 | 60          | 6                |                       |
|                                               |                                 |                                          |   |                                       |   |                                          |    |             |                  |                       |

# FMEA Methodology



## Evaluate the Risk:

- Assign severity, occurrence, and detection ratings to each failure mode:
  - Severity (S):** Impact of the failure (1-10 scale).
  - Occurrence (O):** Likelihood of the failure (1-10 scale).
  - Detection (D):** Likelihood of detecting the failure before it reaches the customer (1-10 scale).
- Calculate the Risk Priority Number (RPN):  
 $RPN = S \times O \times D$   
 $DRPN = S \times O \times D$

## Prioritize Failure Modes:

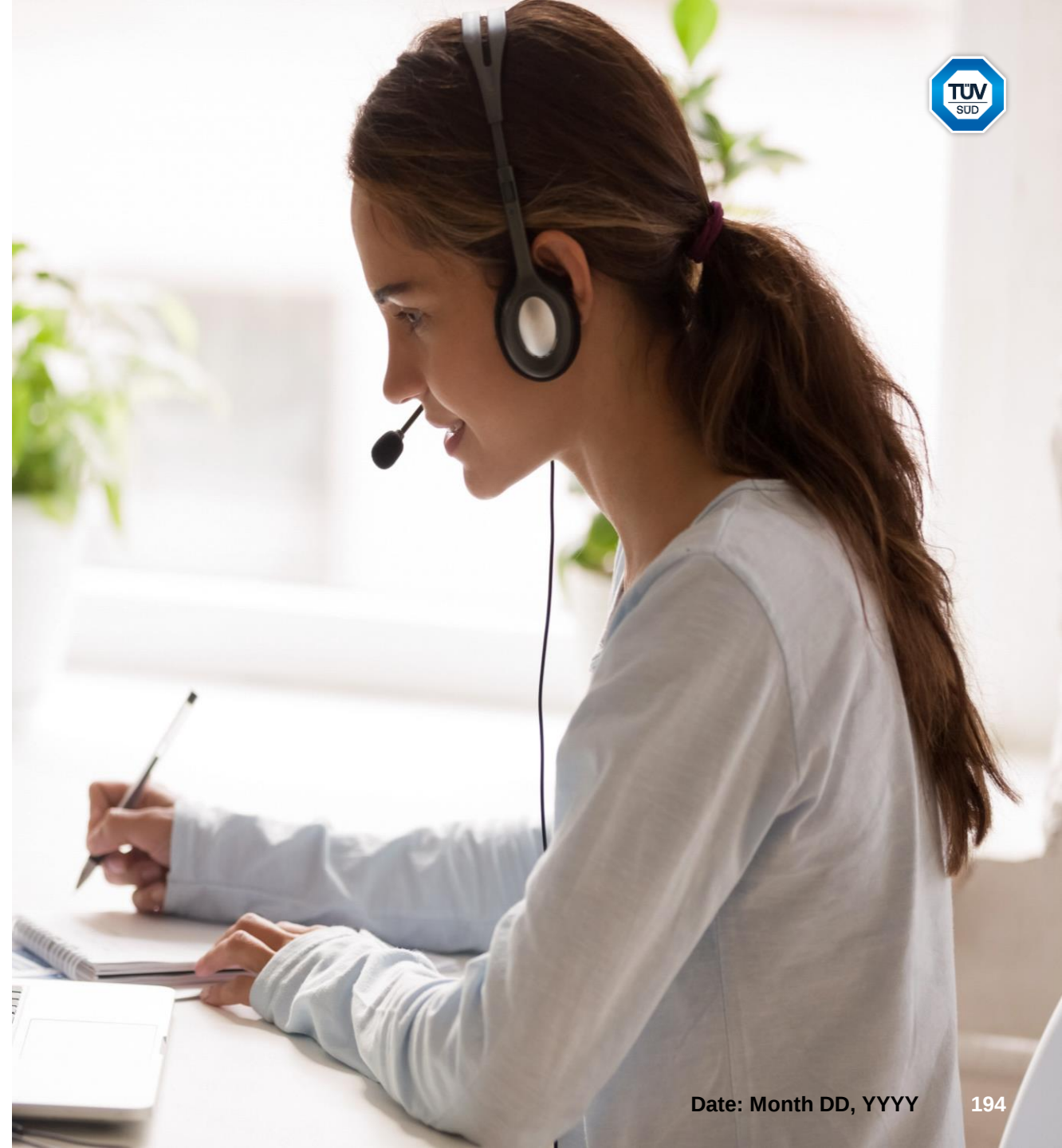
- Rank failure modes based on their RPNs to identify the most critical risks that need attention.

| Function                                      | Potential Failure Mode          | Potential Effects(s) of Failure          | S | Potential Cause(s) of Failure         | O | Current Process Controls                 | D  | RPN | CRI T | Recommended Action(s) |
|-----------------------------------------------|---------------------------------|------------------------------------------|---|---------------------------------------|---|------------------------------------------|----|-----|-------|-----------------------|
| Dispense amount of cash requested by customer | Does not dispense cash          | Customer very dissatisfied               | 8 | Out of cash                           | 5 | Internal low-cash alert                  | 5  | 200 | 45    |                       |
|                                               |                                 | Incorrect entry to demand deposit system |   | Machine jams                          | 3 | Internal jam alert                       | 10 | 240 | 24    |                       |
|                                               |                                 | Discrepancy in cash balancing            |   | Power failure during transaction      | 2 | None                                     | 10 | 160 | 16    |                       |
|                                               |                                 |                                          |   |                                       |   |                                          |    |     |       |                       |
|                                               | Dispenses too much cash         | Bank loses money                         | 6 | Bills stuck together                  | 2 | Loading procedure (riffle ends of stack) | 7  | 84  | 12    |                       |
|                                               |                                 | Discrepancy in cash balancing            |   | Denominations in wrong trays          | 3 | Two-person visual verification           | 4  | 72  | 18    |                       |
|                                               | Takes too long to dispense cash | Customer somewhat annoyed                | 3 | Heavy computer network traffic        | 7 | None                                     | 10 | 210 | 21    |                       |
|                                               |                                 |                                          |   | Power interruption during transaction | 2 | None                                     | 10 | 60  | 6     |                       |
|                                               |                                 |                                          |   |                                       |   |                                          |    |     |       |                       |



# Objectives of FMEA

- to provide a list of equipment and their potential failure modes.
- to describe how equipment fails
- to evaluate the effects of equipment failure on other parts of the process or system in a facility.
- to make recommendations for improving equipment reliability.



# Failure Mode and Effects Analysis (FMEA)

- Establish the physical and operating boundaries of the study.
- Identify and describe each equipment component.
- Beginning at the beginning of a system boundary, evaluate the equipment items in the order that they appear on the process flow diagram.
- List and evaluate all failure modes for each component before proceeding to the next.
- For each failure mode, describe the immediate and surrounding effects and the anticipated effects on other equipment and overall system using a worst-case scenario assuming safeguards do not work.
- Estimate a qualitative rating of likelihood and severity, and by combining these ratings, provide a qualitative risk ranking. Document findings.
- Describe the existing safeguards or procedures that can mitigate the consequences of equipment failure. Document findings.
- List recommendations for corrective actions for further evaluation.

# HAZID



- HAZID is a tool, which was used first in 1992 in an Offshore O&G environment. It utilizes a matrix of possible hazard scenarios, which have to be tested against the design. It is more focused on the architecture (layout) of the system, but it can and has been used to explore unusual events that might not necessarily be identified by a HAZOP. It has targets of about 1000- to 10,000- year return events and as a result the actions have to be assessed by a full QRA.
- A systematic review of the possible causes and consequences of hazardous events . This is a simple but accurate definition. It has been a particular form of Hazard Identification widely used offshore and has proven most useful at Hazard Study (Front-End Engineering Design) where ‘risks’ can be designed out relatively cheaply and also construction.
- While HAZOP is ‘cause’ driven HAZID is ‘consequence’ driven. As with new techniques it took time and usage to develop it to the full potential. Initially it was based upon a HAZID matrix .

| PLANT NAME |                                          | Water Electrolysis Plant                                                                                                               |                                                                                                                                            |                                                                                                                                                |                                                                    | Sheet No. 3-1 |
|------------|------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|---------------|
| Node No.   |                                          |                                                                                                                                        |                                                                                                                                            |                                                                                                                                                |                                                                    | Date:         |
| #          | DANGEROUS DISTURBANCE                    | CAUSES                                                                                                                                 | EXISTING SAFETY MEASURES                                                                                                                   | RECOMMENDATIONS, COMMENTS, ACTIONS                                                                                                             | CORRELATION TO SCENARIO                                            |               |
| 1          | Electrolyte leaks and injury by alkaline | Misoperation and failure of equipment                                                                                                  | • Liquid surface and flow rate monitoring,<br>• Installation of dike, Emergency shower and eyewash,<br>• Connect to tank outlet and gutter | • Work rules creation<br>• Wearing protective equipment such as safety glasses, gloves<br>• Installation of rainwater drain valve and pH meter | A-1<br>C-1,2,5,6                                                   |               |
| 2          | Low pressure hydrogen leaks              | Misoperation and failure of gasholder (V-3201)                                                                                         | • Pressure safety valve<br>• Pressure and amount of displacement monitoring of gas holder (V-3201)                                         | Vacuum safety valve                                                                                                                            | F-2,3,5                                                            |               |
| 3          | High pressure hydrogen leaks             | • Failure of equipment<br>• Damage of piping or equipment                                                                              | • Margin of piping Class<br>• Pressure safety valve<br>• Temperature monitoring at compressor cylinder outlet                              | Oxygen concentration measurement in hydrogen                                                                                                   | F-7,8                                                              |               |
| 4          | Deterioration or damage to membrane      | • Pressure change in the electrolyzer<br>• Flow of the high temperature electrolyte solution<br>• Impurity deposition on the electrode | • Pressure monitoring<br>• Temperature monitoring                                                                                          | Purity monitoring of demineralized water                                                                                                       | C-1,4,5,6,7<br>D-1,2,3,4<br>E-1,2,3,4<br>F-1,3,5<br>G-1<br>I-1,3,5 |               |
| 5          | ...                                      | ...                                                                                                                                    | ...                                                                                                                                        | ...                                                                                                                                            | ...                                                                |               |

# Limitations of PHA



- Can never guarantee that all hazards, causes and consequences have been identified.
- Are only effective if it can safely be assumed that the facility is operated in the manner intended by the designers and in accordance with good practice.
- Are only relevant to the time conducted. Even minor changes may significantly impact facility safety.
- Are subjective and only as good as the collective knowledge, creativity and experience of the team
- Can only be effective and comprehensive if the information available is complete, accurate and up to date.
- May overlook hazards related to material quality and workmanship.
- Are only effective if action is taken to implement the recommendations made during the study.





# Documentation for Decision Making

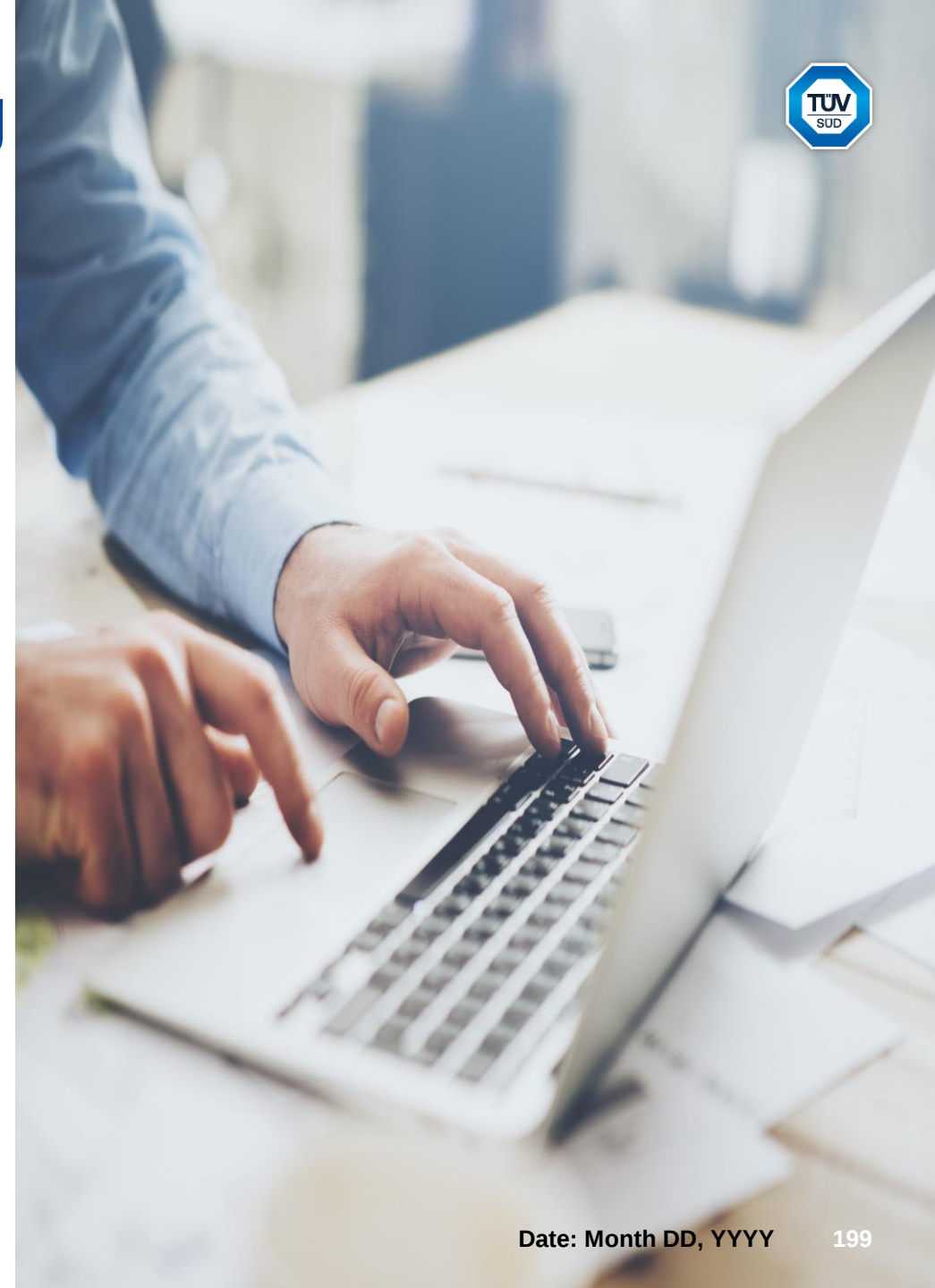
- Preparation of the PHA report is the team leader responsibility. Without adequate documentation, PHA objectives will be difficult for management to achieve and legal liability becomes a risk.
- A question that needs to be resolved with management before the study begins is how much to document. One school of thought is to minimize documentation and save some time by only recording something if a hazard exists. This minimizes time to some extent, but it also minimizes the long-term usability of the results. Complete documentation will provide information for later reference about what was considered, and thus avoid double guessing by later reviewers.
- When deciding how much to document, it is better to document more than less. Computer programs greatly enhance the opportunity to produce a detailed, high quality report in minimal time.



# Documentation for Decision Making



- At a minimum, the report should contain sufficient information to illustrate the quality of the study and document participation. Worksheets with Causes, Consequences and Risk Rankings consistent throughout should be kept. Safeguards need to be documented and Recommendations carefully considered and documented for follow up
- Information contained in PHA reports is a valuable reference for future PHA studies or in the design of future similar processes.
- PHA reports should be maintained at the facility for the life of the process for reference and audit purposes.
- PHA reports are confidential and should be maintained as such.



# Worksheet Report



- Worksheets need to be concise, but complete in detail. For example, the location, line, equipment and valve numbering for each recommendation must be documented.
- Worksheets and Action Sheets are business documents that can be used in a court of law.
- The language used in documenting the study needs to be carefully chosen.
  - Do not use expressions that are personal opinions or legal opinions or conclusions.
  - Do not make judgments about quality of work or conduct.
  - Do not use words with negative connotations such as, “catastrophic” or “fatal.”
  - Do not use words that constrain management to only one action (there may be more suitable alternatives).

## HAZID Worksheet

| Node            |       |                             |           |          |                |
|-----------------|-------|-----------------------------|-----------|----------|----------------|
| Area/Equipment  |       |                             |           |          |                |
| Hazard/Incident | Cause | Hazardous Event/Consequence | Safeguard |          | Recommendation |
|                 |       |                             | Hardware  | Software |                |
|                 |       |                             |           |          |                |
|                 |       |                             |           |          |                |
|                 |       |                             |           |          |                |

# Completed Reports



- Executive Summary of Proceedings
- Introduction
- Process Description
- Study Scope and Objectives
- Hazard Analysis Technique
- Risk Matrix
- Node or System/Subsystem List
- Worksheets
- Prioritized Recommendations
- Drawings and other references used in the study

## Table of Contents

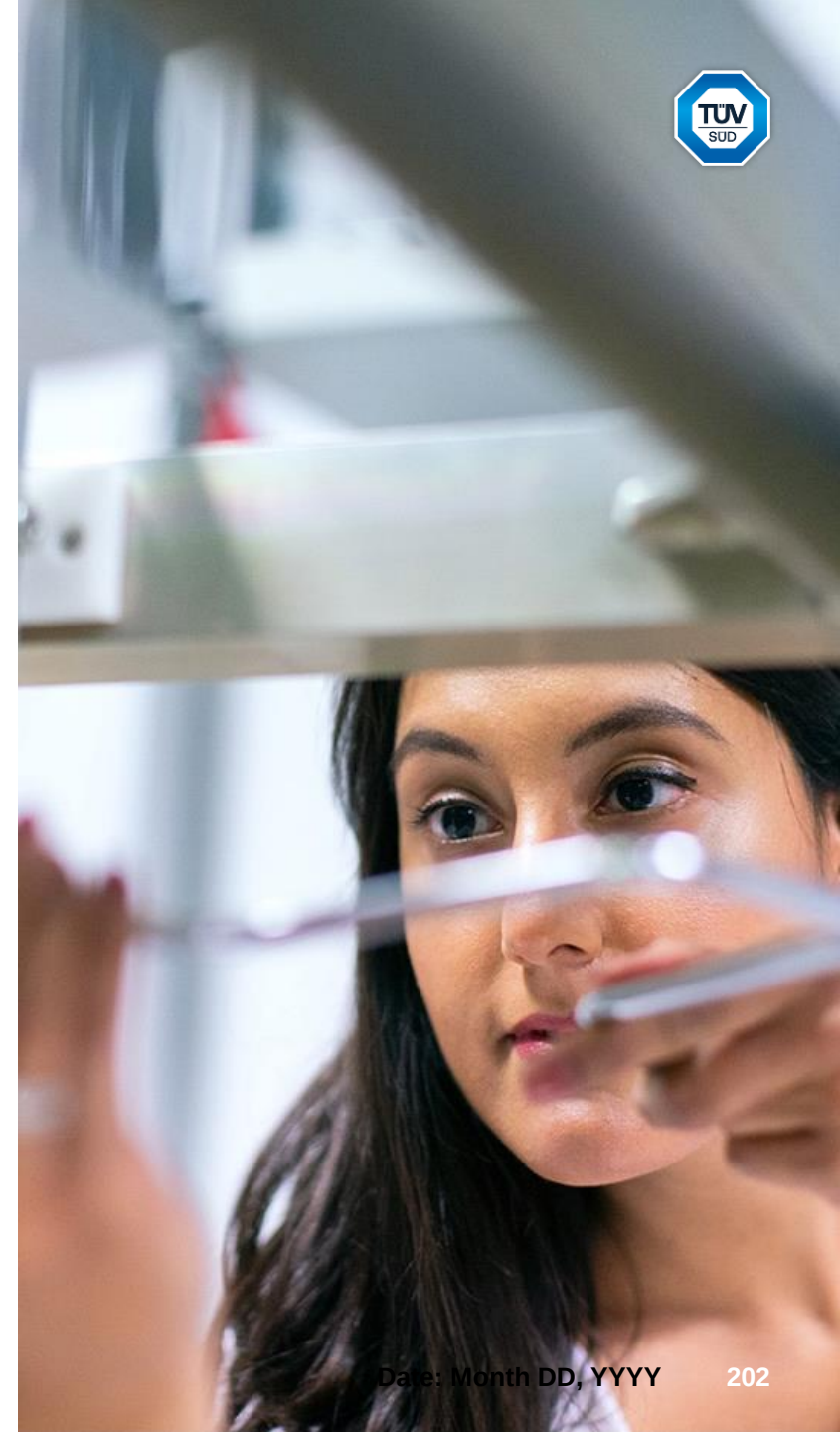
|                                                                         |           |
|-------------------------------------------------------------------------|-----------|
| <b>1. EXECUTIVE SUMMARY</b> .....                                       | <b>3</b>  |
| <b>2. PROCESS DESCRIPTION</b> .....                                     | <b>3</b>  |
| <b>3. HAZOP OBJECTIVE AND SCOPE OF WORK</b> .....                       | <b>4</b>  |
| 3.1 HAZOP Objectives .....                                              | 4         |
| 3.2 HAZOP Scope.....                                                    | 4         |
| <b>4. METHODOLOGY</b> .....                                             | <b>4</b>  |
| <b>5. ABBREVIATIONS</b> .....                                           | <b>6</b>  |
| <b>6. DEFINITIONS</b> .....                                             | <b>7</b>  |
| <b>7. HAZOP Team Members / Participants</b> .....                       | <b>8</b>  |
| <b>8. GUIDELINES TO RESPONDING TO HAZOP STUDY RECOMMENDATIONS</b> ..... | <b>9</b>  |
| <b>9. STUDY RECOMMENDATIONS</b> .....                                   | <b>11</b> |
| <b>10. HAZOP FOLLOW-UP</b> .....                                        | <b>12</b> |
| <b>11. HAZOP RISK MATRIX</b> .....                                      | <b>12</b> |
| <b>12. REFERENCES</b> .....                                             | <b>12</b> |
| <b>13. REFERENCE DOCUMENTS</b> .....                                    | <b>12</b> |
| <b>APPENDIXES</b> .....                                                 | <b>13</b> |
| <b>APPENDIX A. HAZOP TEAM ATTENDANCE LIST</b> .....                     | <b>14</b> |
| <b>APPENDIX II: HAZOP GUIDEWORDS</b> .....                              | <b>15</b> |
| <b>APPENDIX C: - Nodes</b> .....                                        | <b>16</b> |
| <b>Appendix-D: Risk Ranking</b> .....                                   | <b>17</b> |
| <b>APPENDIX- E HAZOP WORKSHEETS</b> .....                               | <b>18</b> |



# Summary

What we have learned in the module

- What If Analysis
- What If Analysis STEPS
- FMEA
- Steps in an FMEA
- Limitations of PHA



# Exercise 6 - Questions



Q1) What If can be used at any time for new or existing facilities. Requires an experienced team and adequate preparation

- A. True
- B. False

Q2) -..... is not strictly speaking a hazard identification technique, but it provides an important source of hazard information because it documents and describes all the ways in which individual pieces of equipment can fail and the effects of such failure on a facility

- A. HAZOP
- B. What if
- C. FTA
- D. FMEA

# Exercise 6 - Questions



Q3) .....is Questions can also focus on specific consequences such as process safety, operating procedures, human error or environmental safety. Does not easily generate operability information, Questions are applied to existing P&IDs and process descriptions

- A. HAZOP
- B. What if
- C. FTA
- D. ETA
- E. HAZID

# Exercise 6 - Questions



Q4) Process Hazard Analysis (PHA's) only uses two methodologies: the “WHAT IF” or the “HAZOP”?

A. True

B. False

Q5) What is the limitation of PHA ?



# Note



# Any Question?



**Follow us on:**



[tuvsud.com](https://www.tuvsud.com)  
[info@tuvsud.com](mailto:info@tuvsud.com)

# CERTIFIED PHA - HAZOP LEADER LEADERSHIP



01

**Module 1**  
INTRODUCTION

02

**Module 2**  
PROCESS SAFETY MANAGEMENT

03

**Module 3**  
HAZOP

04

**Module 4**  
REHAZOP & LOPA

05

**Module 5**  
Checklists

06

**Module 6**  
WHAT IF & FMEA

07

**Module 7**  
LEADERSHIP

08

**Module 8**  
BOWTIE ANALYSIS



# 7 LEADERSHIP

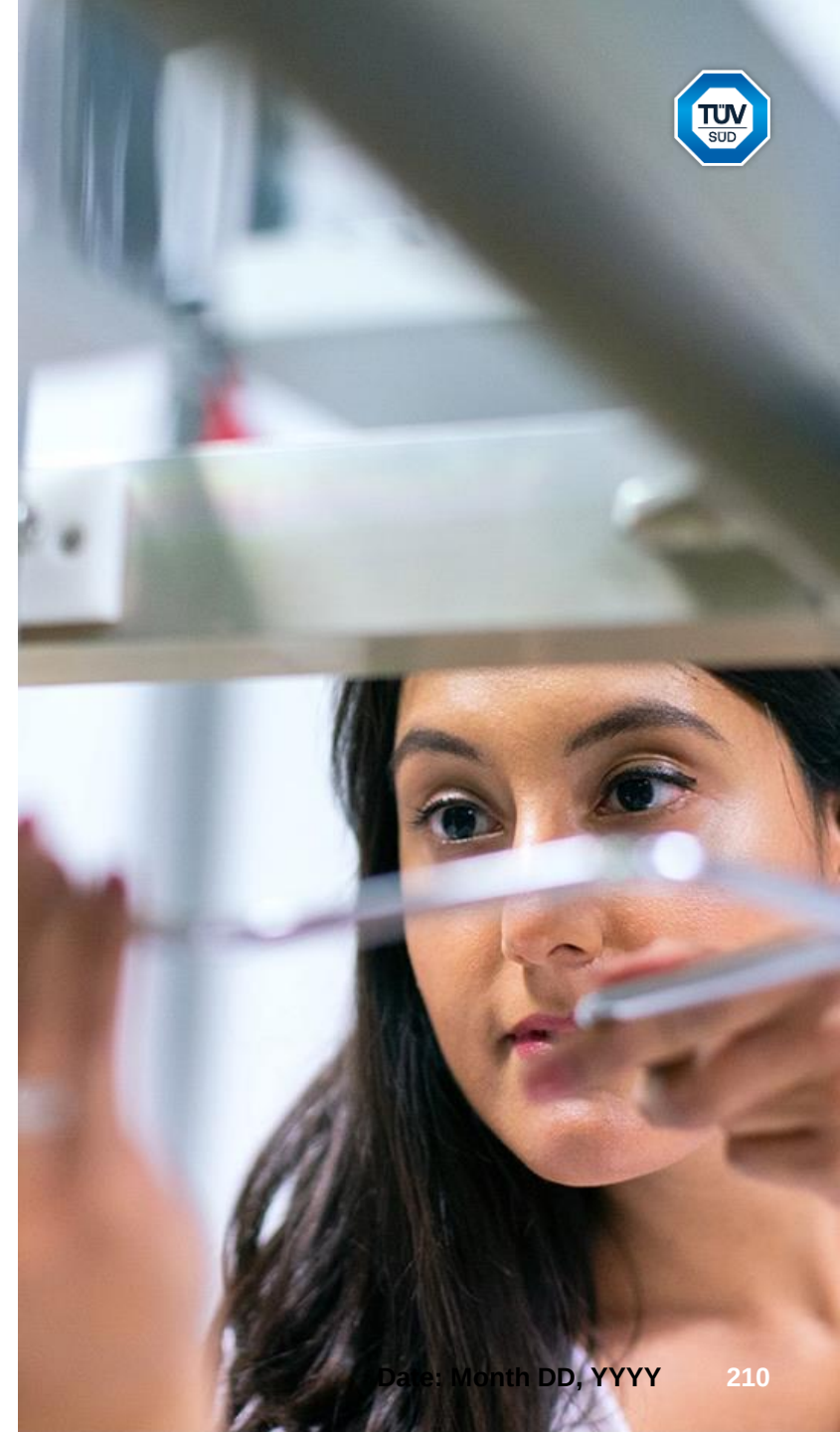


# Module 7

## LEADERSHIP

In this module

- PHA Leadership Responsibilities
- PHA Quality Problems
- Getting the Best From Your Team
- Leadership Styles



# PHA LEADERSHIP

- Formal PHA leadership training or documented experience as a team leader
- Leadership and conflict resolution training if possible
- Experience as a team member
- Strong ability to interpret engineering drawings
- No day to day responsibility for the process being studied
- Extensive engineering and safety experience



# PHA Leadership Responsibilities

- Formal PHA leadership training or documented experience as a team leader
- Leadership and conflict resolution training if possible
- Experience as a team member
- Strong ability to interpret engineering drawings
- No day to day responsibility for the process being studied
- Extensive engineering and safety experience





# PHA Quality Problems

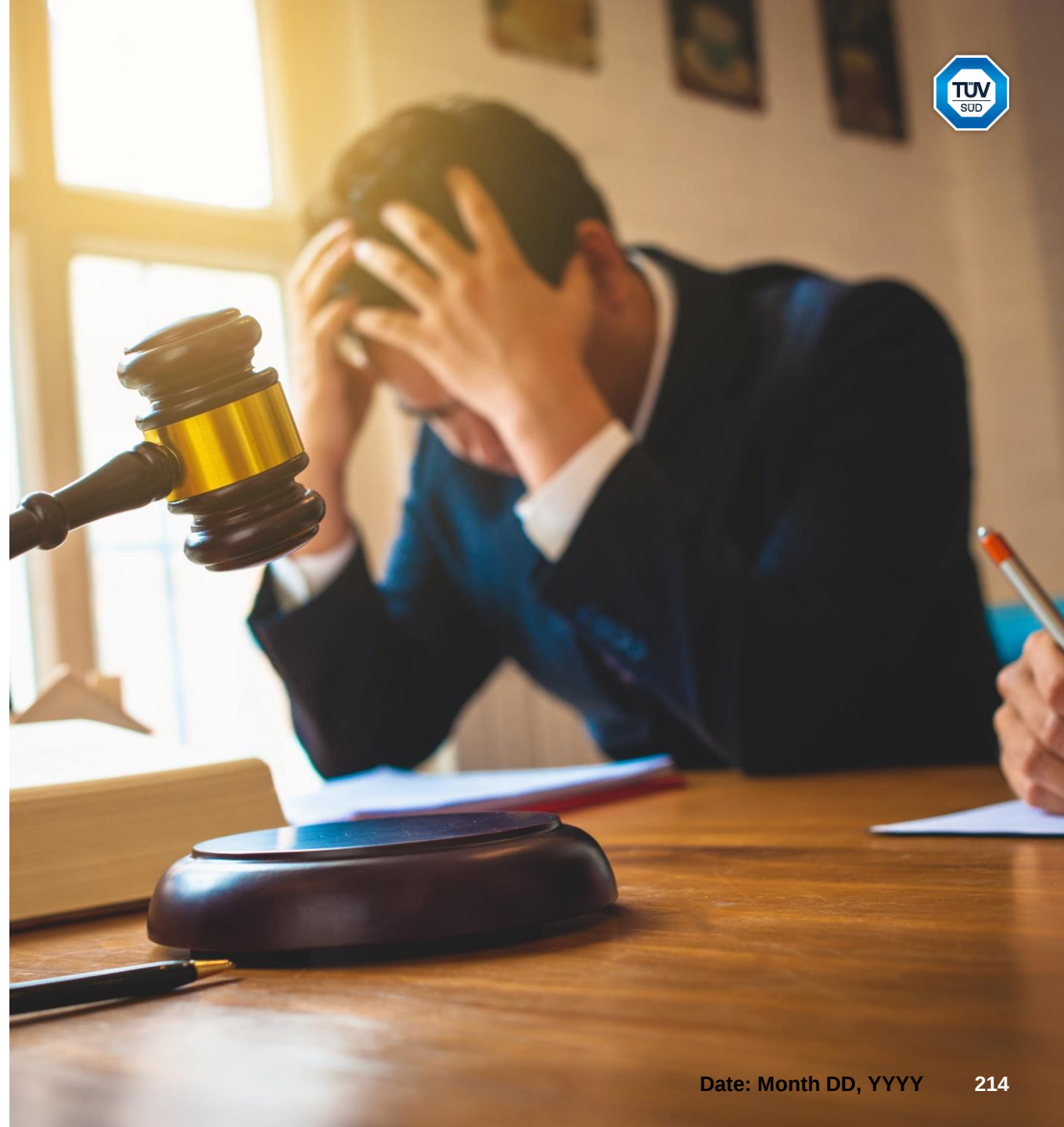
- Inappropriate management expectations
- Inadequate time allotted for study
- Poor scope definition
- Inaccurate or incomplete data
- Inadequate documentation
- Inadequate team guidance
- Distractions and poor team motivation
- Uncomfortable and inadequate meeting facility
- Lack of follow up on study results





# Getting the Best From Your Team

- Aggressor
- Dominator
- Blocker
- Recognition Seeker
- Special Interest Pleader
- Speed Freak
- MR. Re-Engineer It
- Joker
- Ho Hum Person



# Leadership Styles

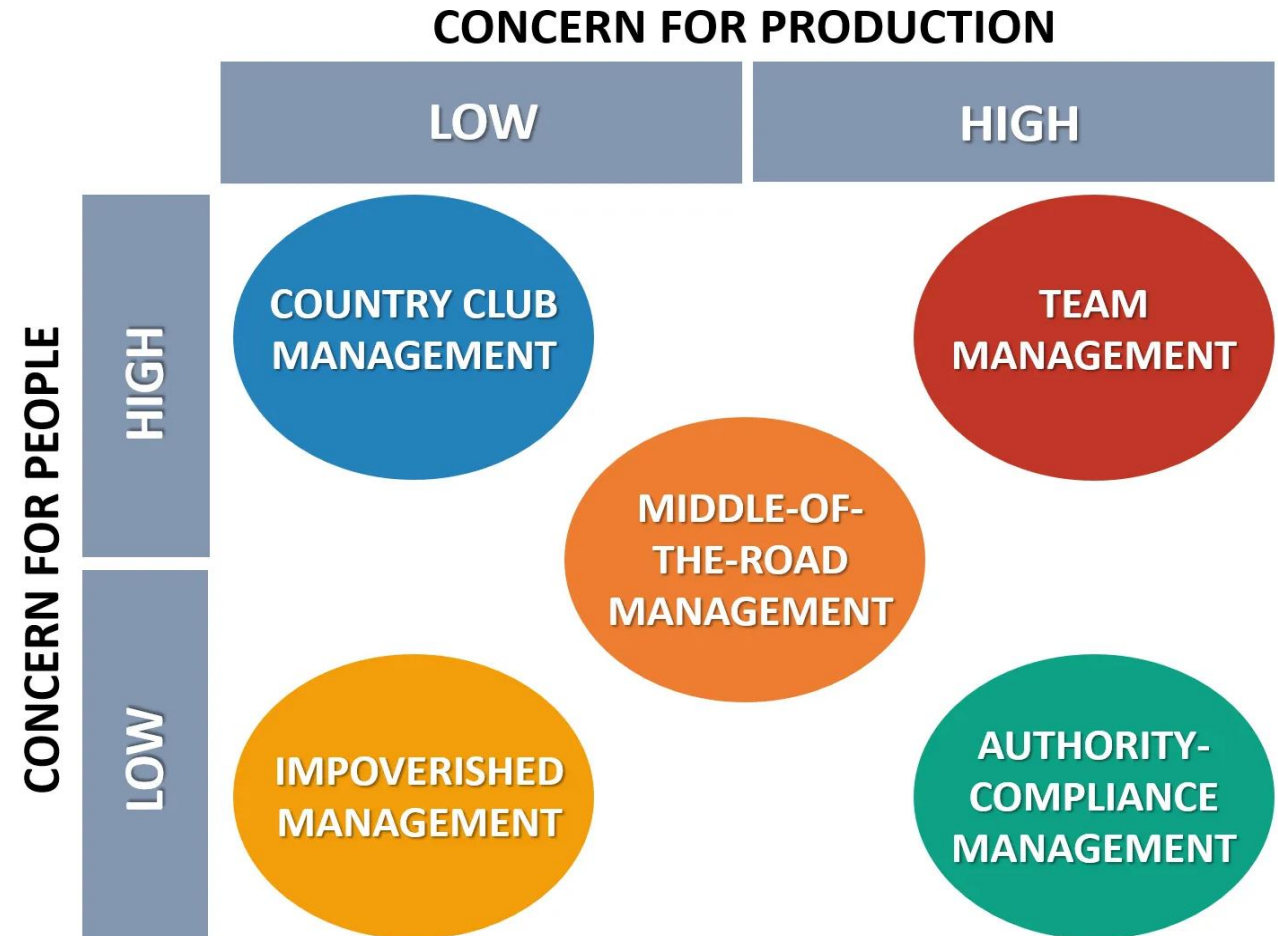
- Everyone knows that strong leadership is central to business success. To motivate teams and harness talent, leaders must effectively communicate with, delegate to, and mentor employees, while inspiring them to pursue the company's business purpose and mission.
- This requires the flexibility to switch among different types of leadership styles – which doesn't always come instinctively or easily.



# Leadership Styles



- People tend to employ leadership styles that are rooted in their innate preferences, personalities, and backgrounds. This isn't a bad thing; knowing which leadership style naturally works best for you is part of being a good leader. But rigidly sticking to one style can stifle company and employee growth. To enhance leadership effectiveness, it's crucial to develop a malleable style that integrates various leadership techniques, adapting to new situations as they arise.





# Leadership Styles

- What constitutes a good manager? Based on behavioural research studies on leadership and management (e.g. Ohio State Studies and Michigan Studies), two basic management behaviours can be identified as important: task-oriented behaviour and people-oriented behaviour. Even though these two factors are not the only important management behaviours, concern for both the task and the people must be shown at some reasonable level.

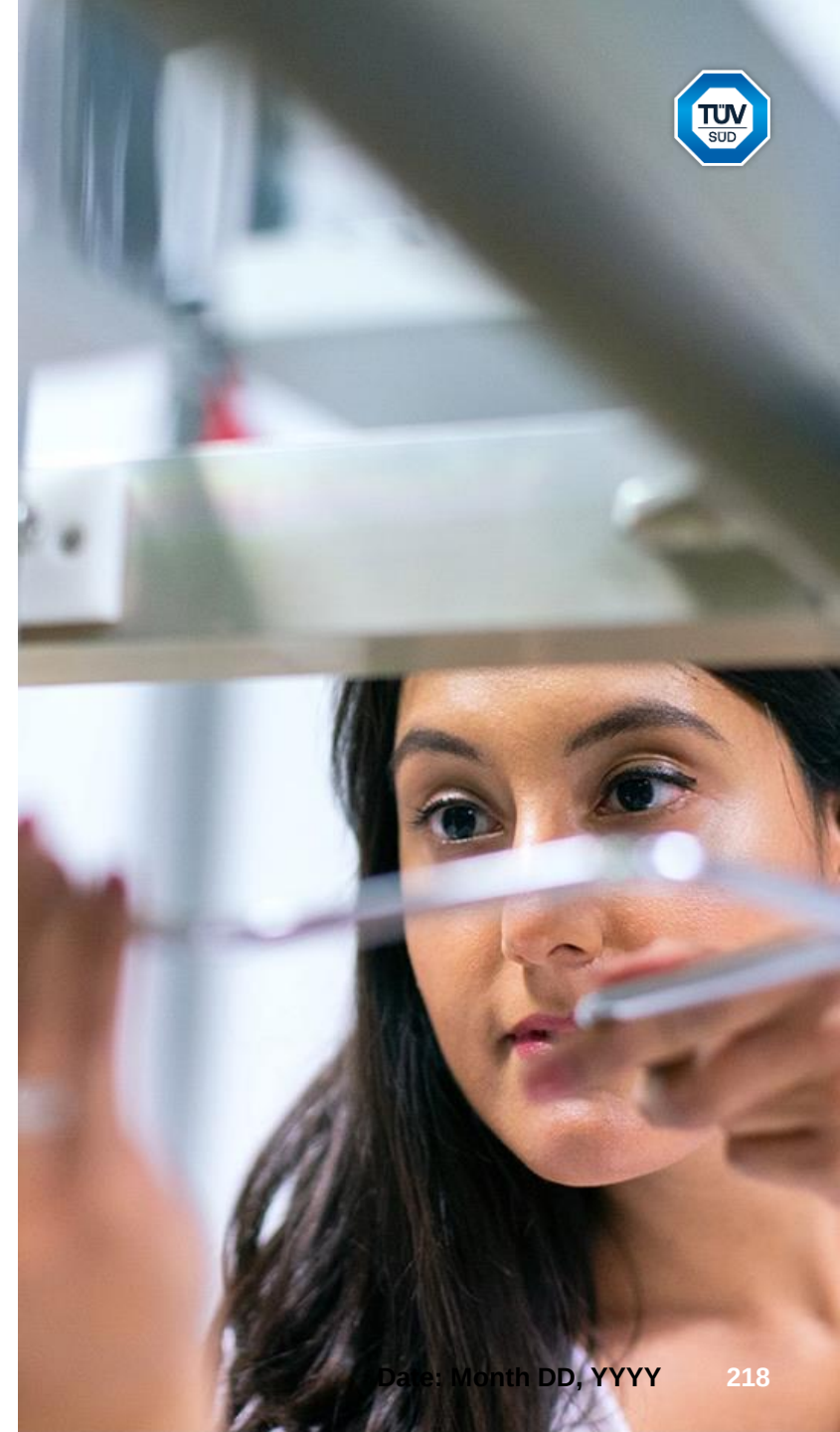




# Summary

What we have learned in the module

- PHA Leadership Responsibilities
- PHA Quality Problems
- Getting the Best From Your Team
- Leadership Styles



# Exercise 7 - Questions



Q1) Country Club Management concern for production rather than people

A. True

B. False

Q2) As a HAZOP leader, how do you deal with conflict issue between team members? and how to control the discussion ?

Q3) What is the optimum number of team members to conduct the HAZOP study? And why?

# Note



# Any Question?



**Follow us on:**



[tuvsud.com](https://tuvsud.com)  
[info@tuvsud.com](mailto:info@tuvsud.com)



# CERTIFIED PHA - HAZOP LEADER

## BOWTIE ANALYSIS



01

**Module 1**  
INTRODUCTION

02

**Module 2**  
PROCESS SAFETY MANAGEMENT

03

**Module 3**  
HAZOP

04

**Module 4**  
REHAZOP & LOPA

05

**Module 5**  
Checklists

06

**Module 6**  
WHAT IF & FMEA

07

**Module 7**  
LEADERSHIP

08

**Module 8**  
BOWTIE ANALYSIS

# 8

# BOWTIE ANALYSIS

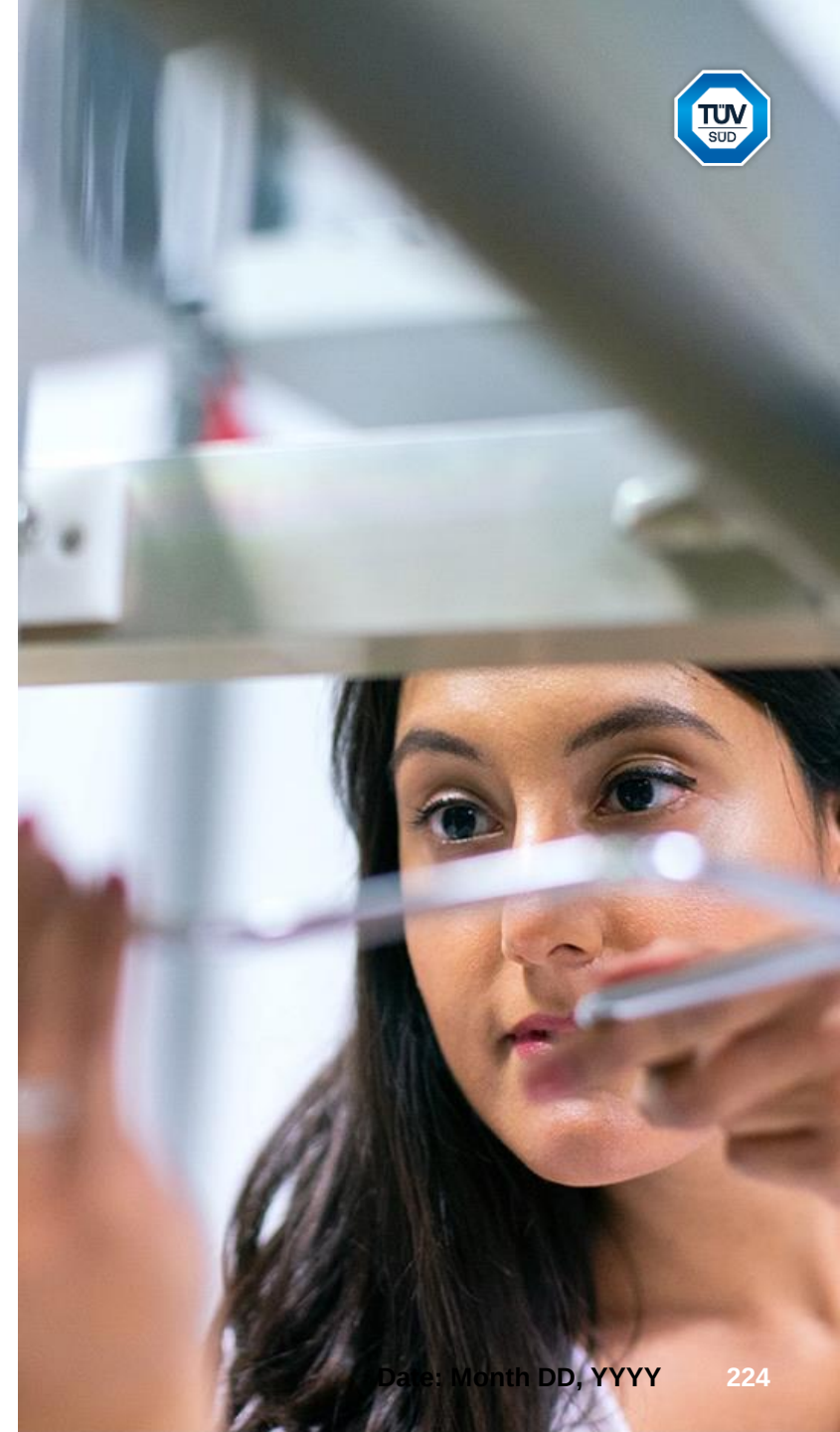


# Module 8

## BOWTIE ANALYSIS

In this module

- Bow-Tie Definitions
- WHAT IS A BARRIER?
- WHAT IS A VALID BARRIER?
- Steps to describe a barrier



# BOWTIE ANALYSIS

- **Hazard:**

A Hazard is a situation or dormant potential which could lead to an Event when a Cause is activated.(Business hazards are unavoidable)

- **Event:**

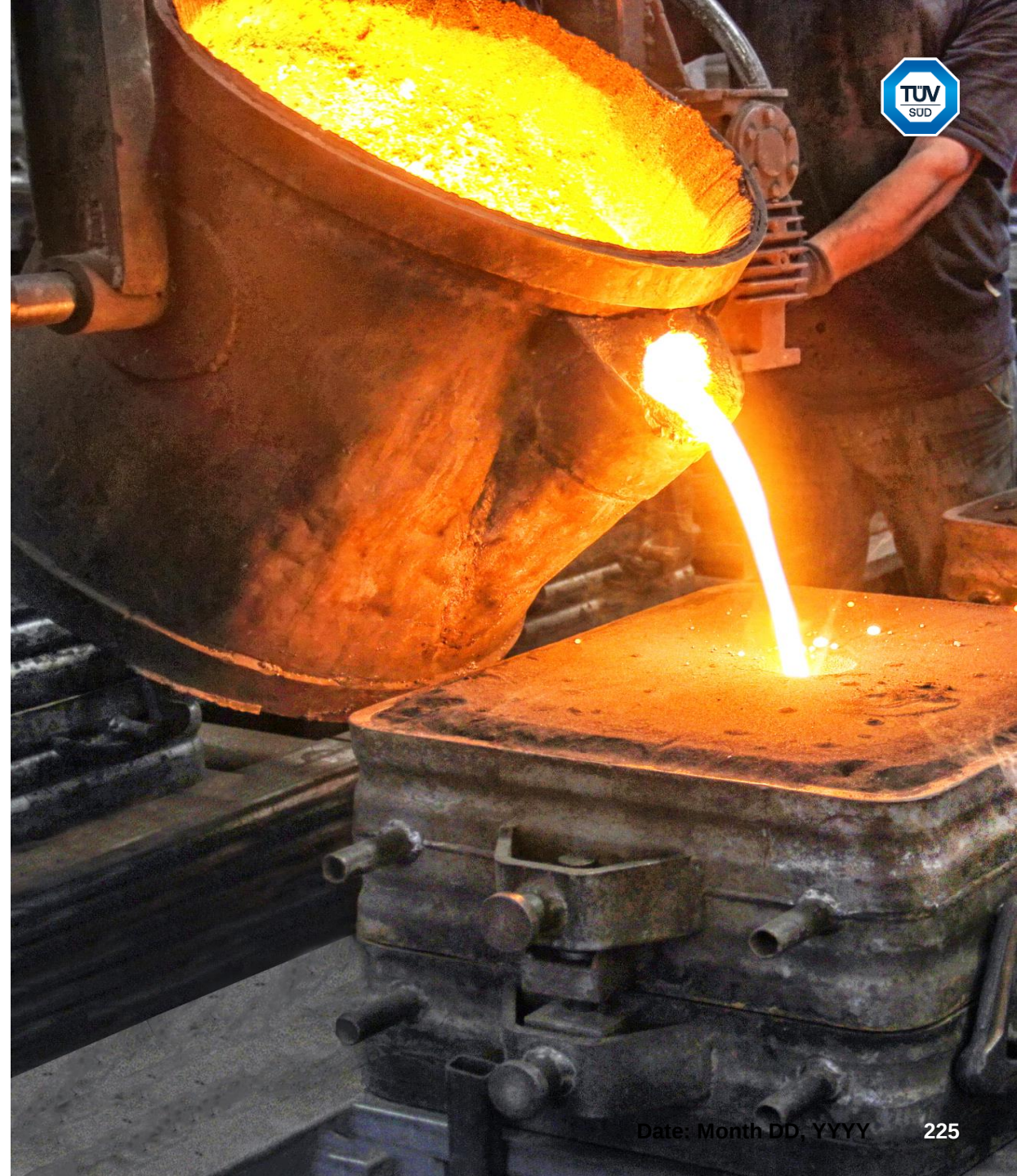
A Event is the moment when control is lost over the Hazard. There is no damage or negative impact yet, but it is imminent.

- **Cause:**

Causes are whatever will lead to an Event in the presence of a Hazard.

- **Barriers:**

Barriers will prevent the Event occurring in the presence of the Cause

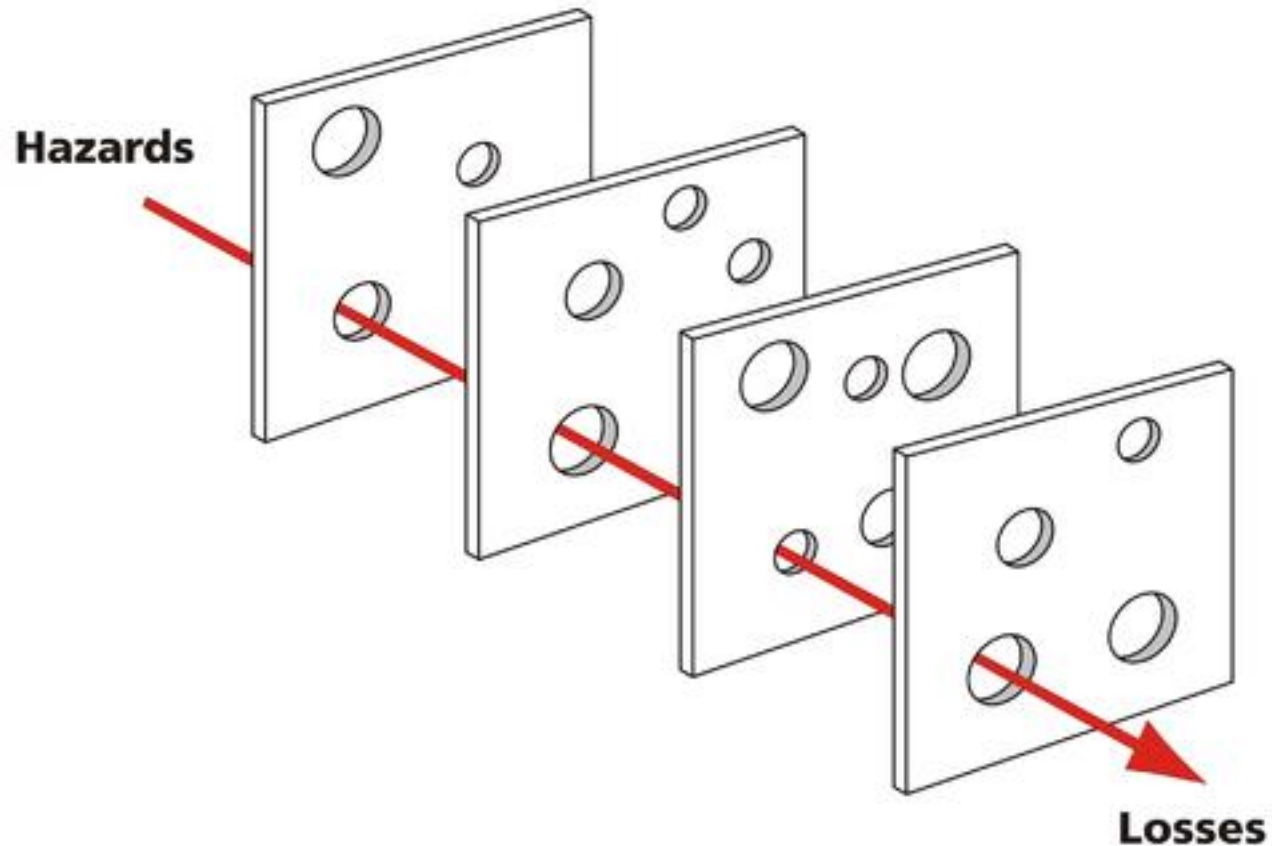




# WHAT IS A BARRIER?



- Dictionary Definition : Something that blocks or is intended to block passage, hinder movement or action
- Our Definition: A protective measure put in place to prevent or limit the harm from a Major Accident Hazards



# WHAT IS A BARRIER?



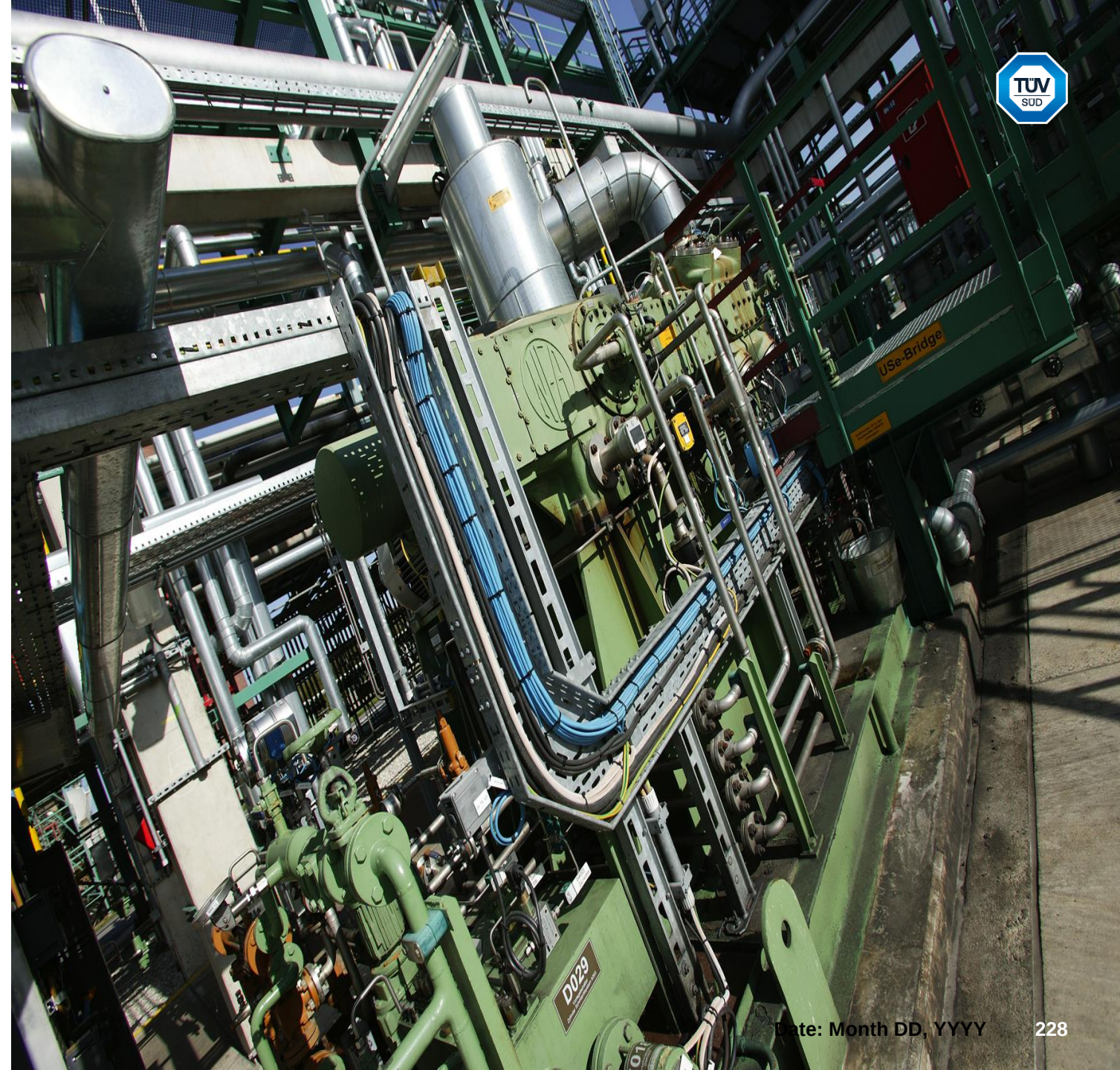
- In order for a Barrier to be considered valid it must be: effective, independent and auditable:
- **Effective:** The Barrier prevents the consequence when it functions as designed (i.e. big enough, fast enough, strong enough).
- **Independent:** The Barrier also needs to be independent of the initiating event.
- **Auditable:** The Barrier can be evaluated to verify that it can operate correctly when it is called upon.





# WHAT IS A BARRIER?

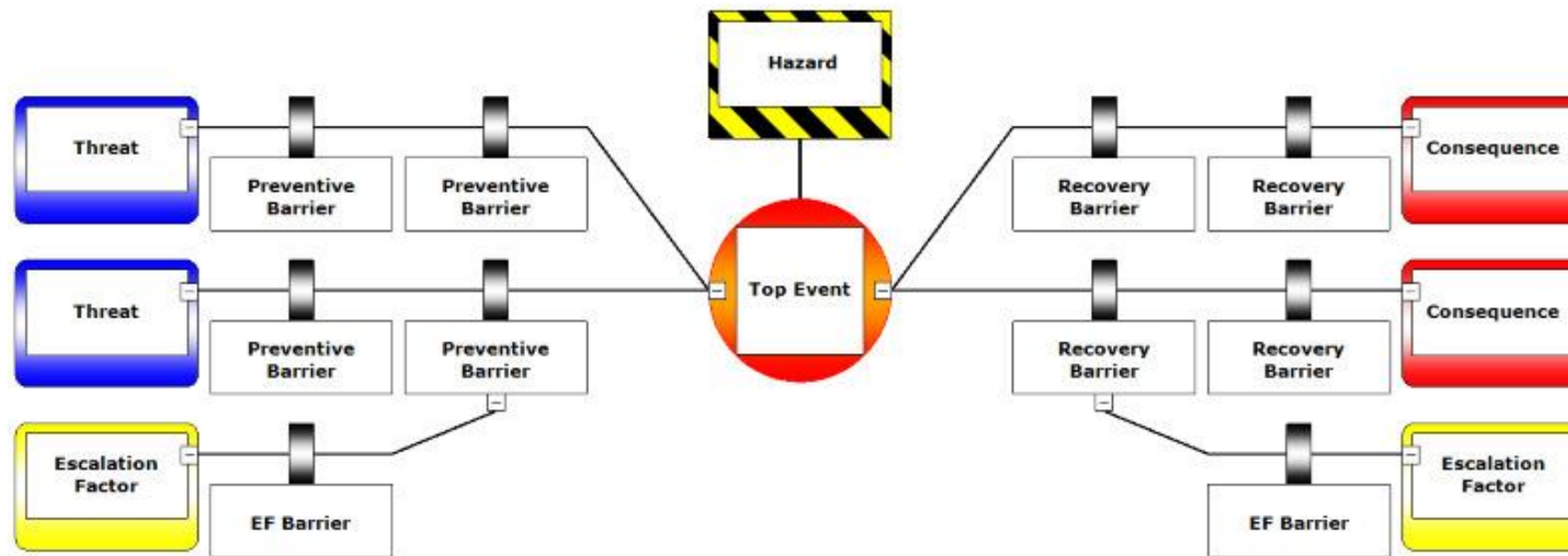
- Independent means that it has no common failure modes amongst other barriers on the same cause or consequence line and no common failure mode with the corresponding cause
- A prevention barrier is described as 'fully functional' if it is capable of preventing a cause developing into a risk event
- A mitigation barrier is described as 'fully functional' if it is capable of either completely mitigating the consequences of a risk event, or reduces the severity





# Bowtie methodology

- The bowtie methodology is used for risk assessment, risk management and (very important) risk communication. The method is designed to give a better overview of the situation in which certain risks are present; to help people understand the relationship between the risks and organizational events.

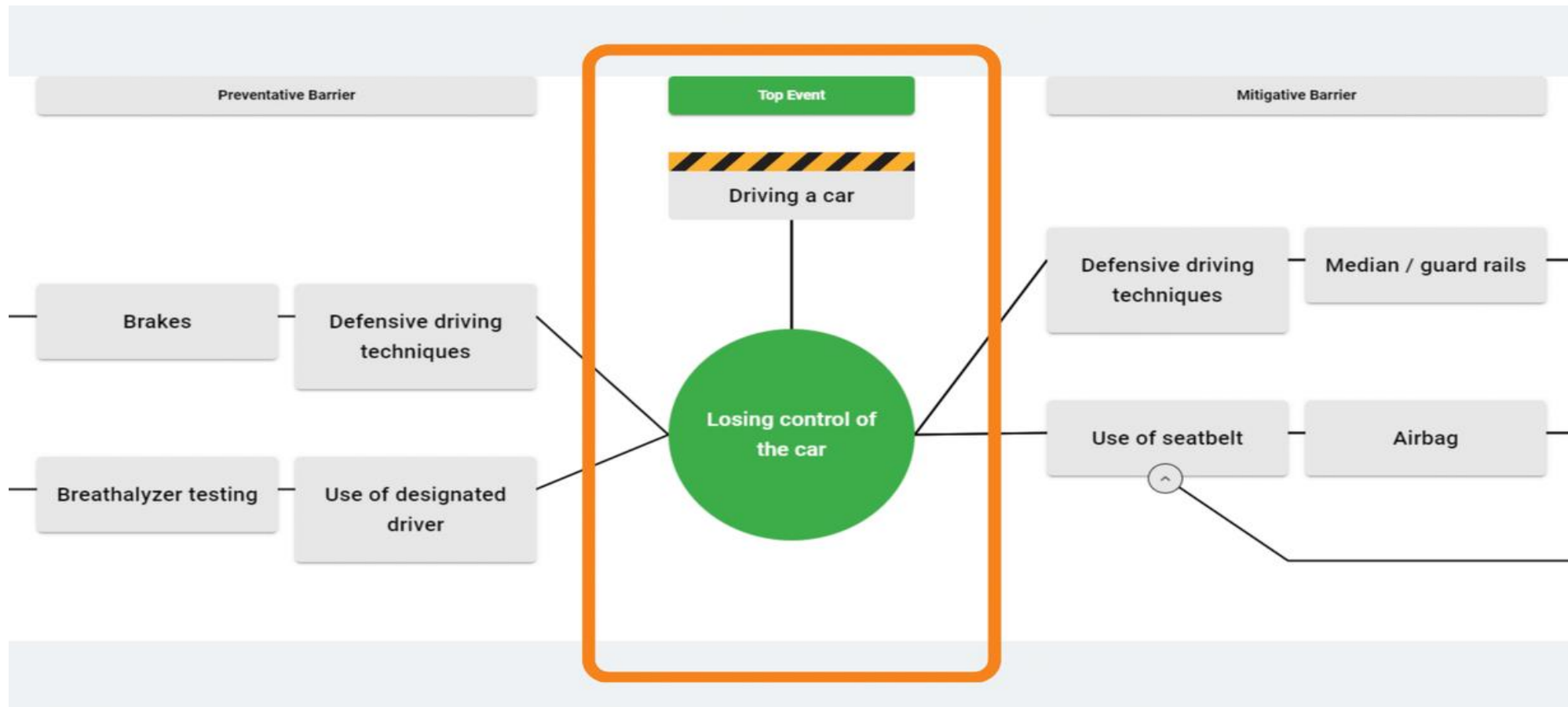




# Bowtie methodology

## Identify hazard

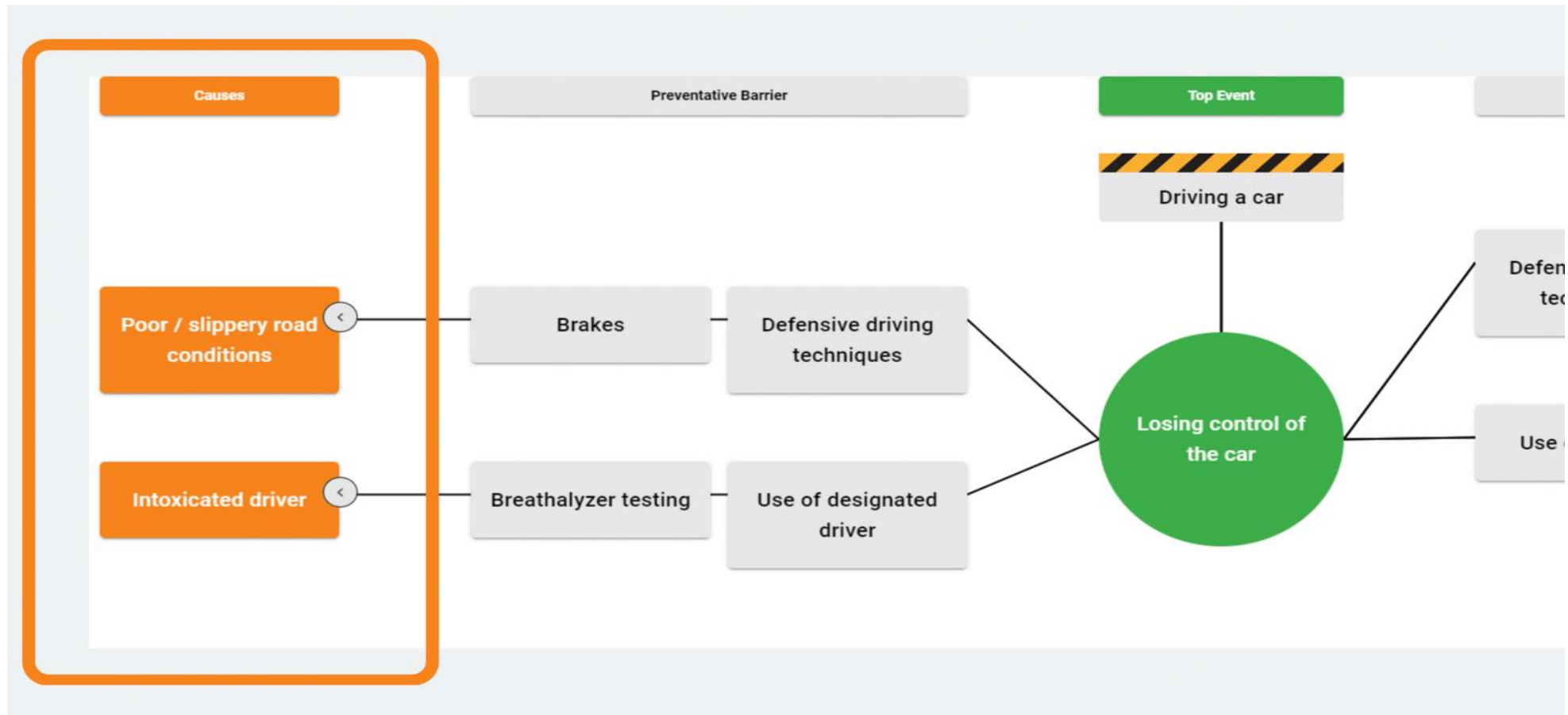
- The top event in a bowtie diagram is the event that triggers the analysis.
- It could be anything from a system crash to an event that has the potential to cause significant damage.



# Bowtie methodology

## Identify threats

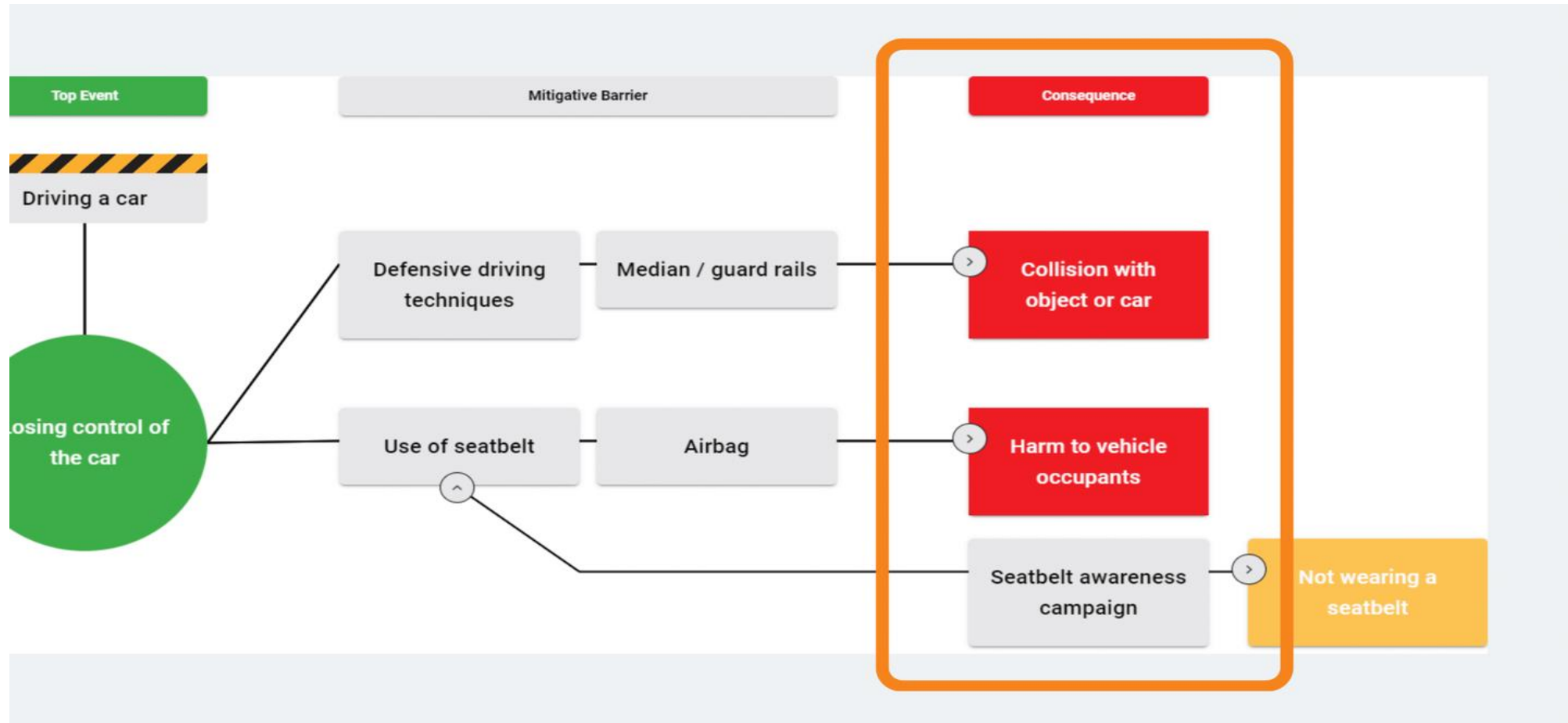
- The threats in a bowtie diagram are the potential factors that could lead to the event.
- These could be anything from system malfunctions to human error.



# Bowtie methodology

## Evaluate consequences

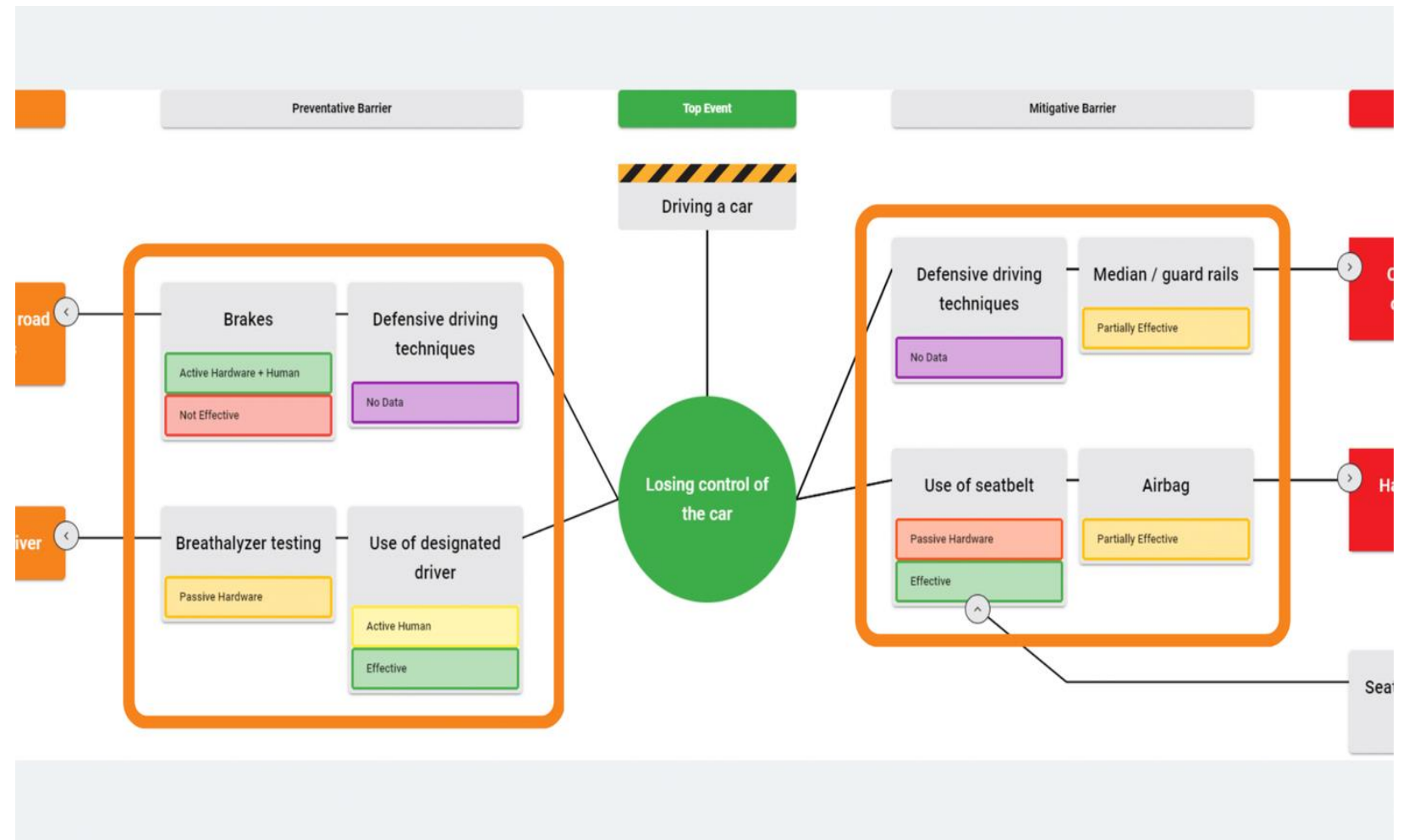
- The potential consequences for the top event could include damage to the environment, injuries to staff or customers, loss of business and even loss of life.



# Bowtie methodology

## Identify barriers

The barriers in a bowtie diagram are the measures that have been taken to address the causes and mitigate the damage caused by the consequences. This can include installing additional safety measures and training staff in how to handle emergency situations. By understanding the barriers and how they have been implemented you can ensure that any damage caused by a top event is limited.

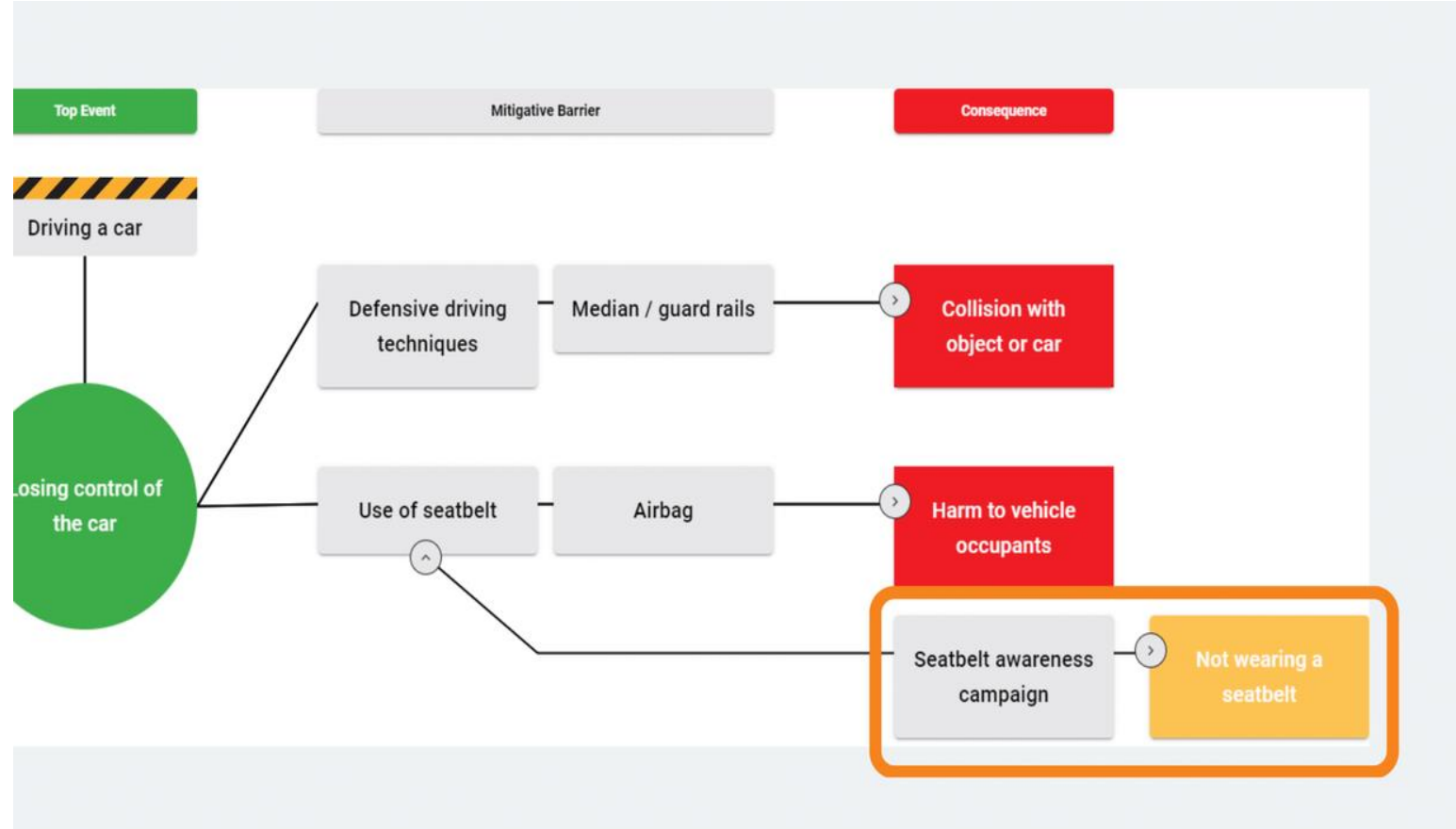




# Bowtie methodology

## Identify escalation factors

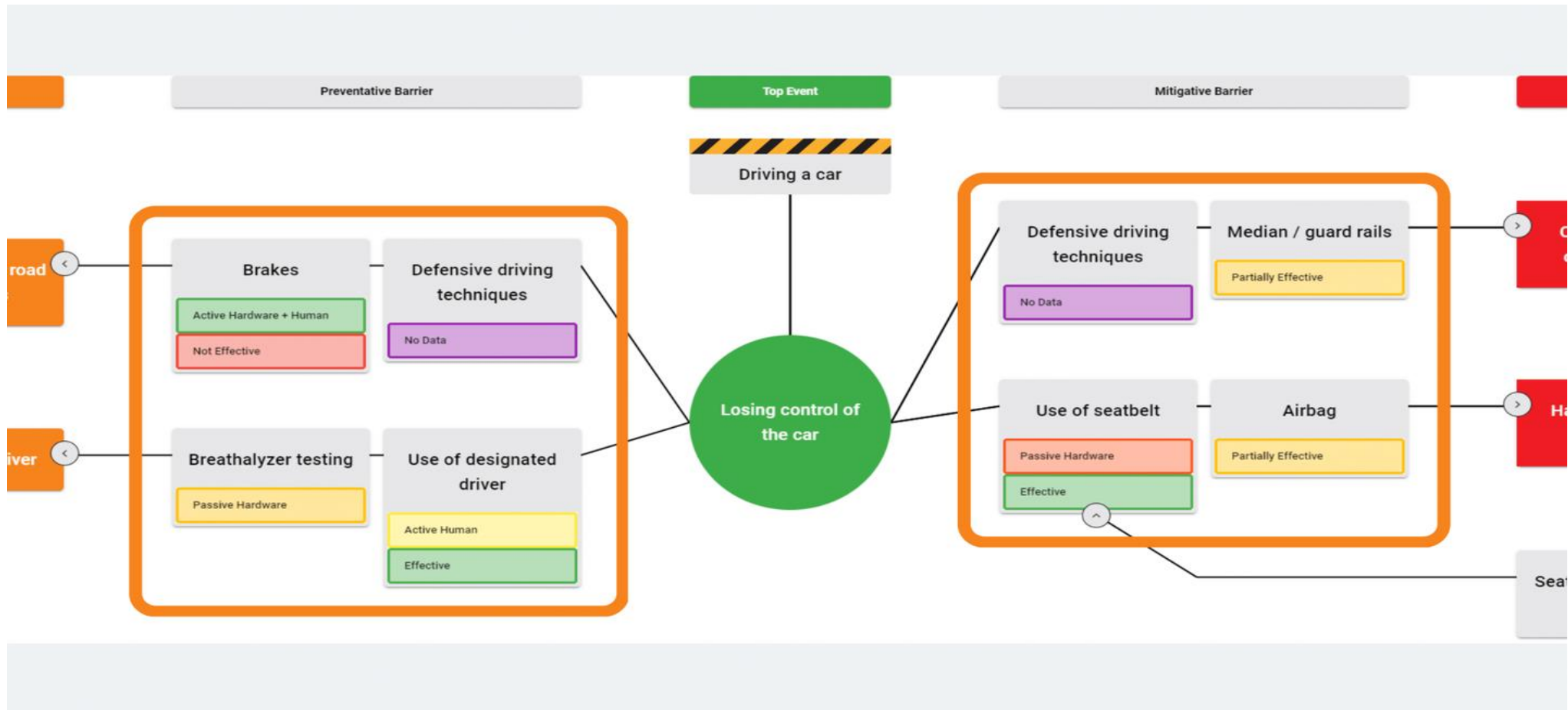
- Escalation factors should be used sparingly, representing only barrier failure modes presenting a major threat.
- Barriers to escalation factors work in the same way as barriers to causes and consequences. From our example, a barrier to an escalation factor of not wearing a seatbelt would be a seatbelt campaign by the government, highlighting the risks of not using a seatbelt.



# Bowtie methodology

## Barrier Effectiveness

- effective the barrier is and what are the possible influences of a cause or consequence are. By color coding how effective the barrier condition is, it gives a clear indication of where adjustments need to be made



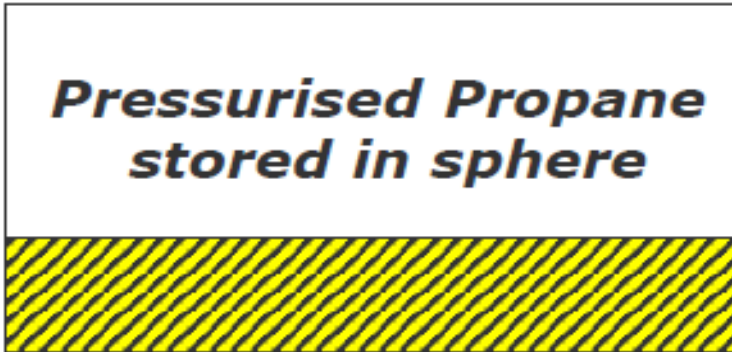
# Examples and useful rules for quality in bow ties



- Hazard is an operational, activity or materials with the potential to cause harm
- “What you are trying to control”

## Hazards should

- Be specific
- For the hazard in its controlled state
- Can also include:
  - Situational context
  - Indication of scale



# Effectiveness vs condition

## Effectiveness



- The initial effectiveness of the barrier – “how well each barrier performs”
- Design intent / performance standards set required effectiveness:
  - Functionality
  - Reliability, availability and survivability
- Some barriers will be naturally more effective than others

## Condition / state

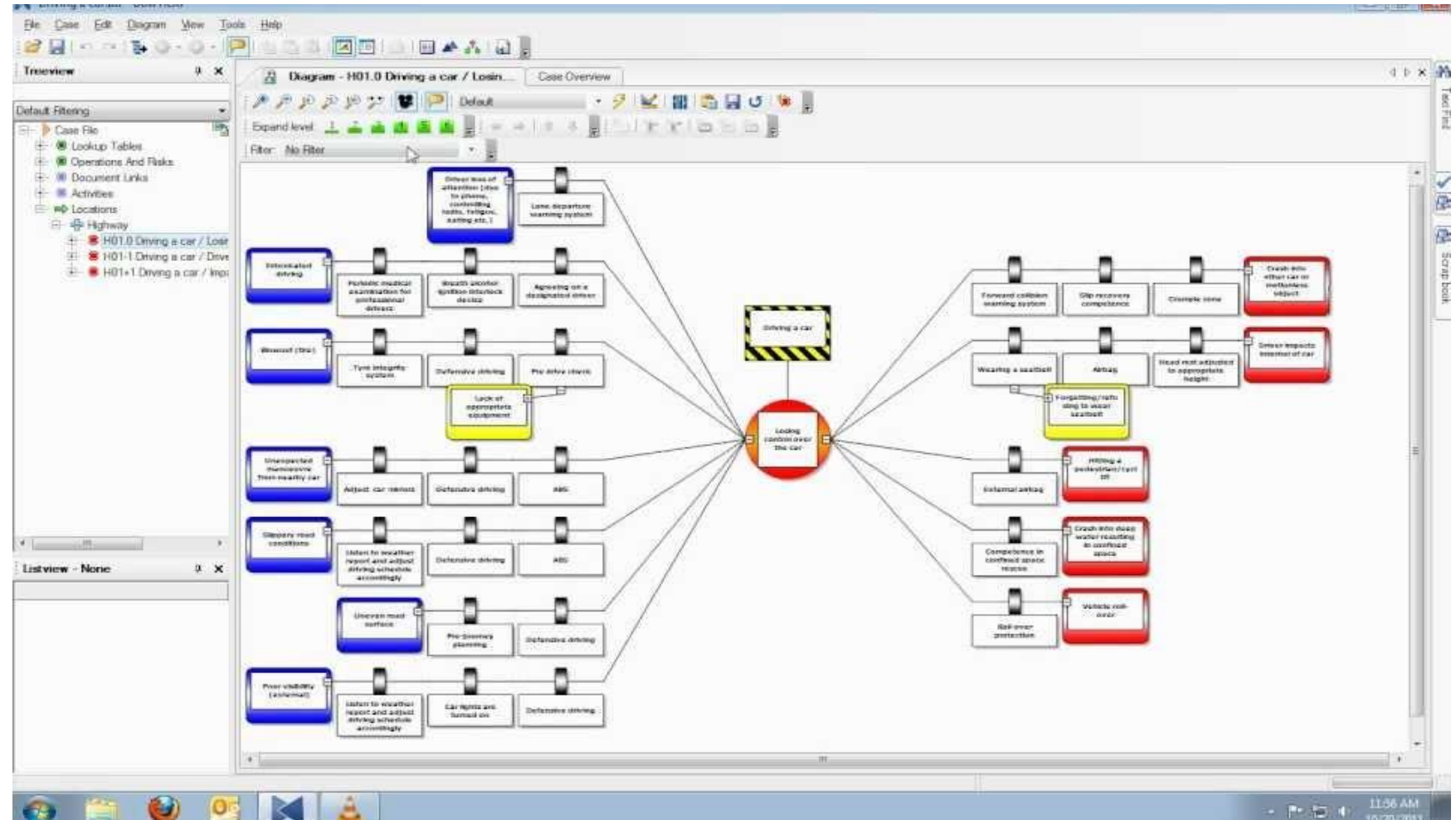


- How well is the barrier performing vs its required performance (i.e. its design intent / performance standards)?
- Degradation affects the barrier condition



# Bow Tie workshop guidelines

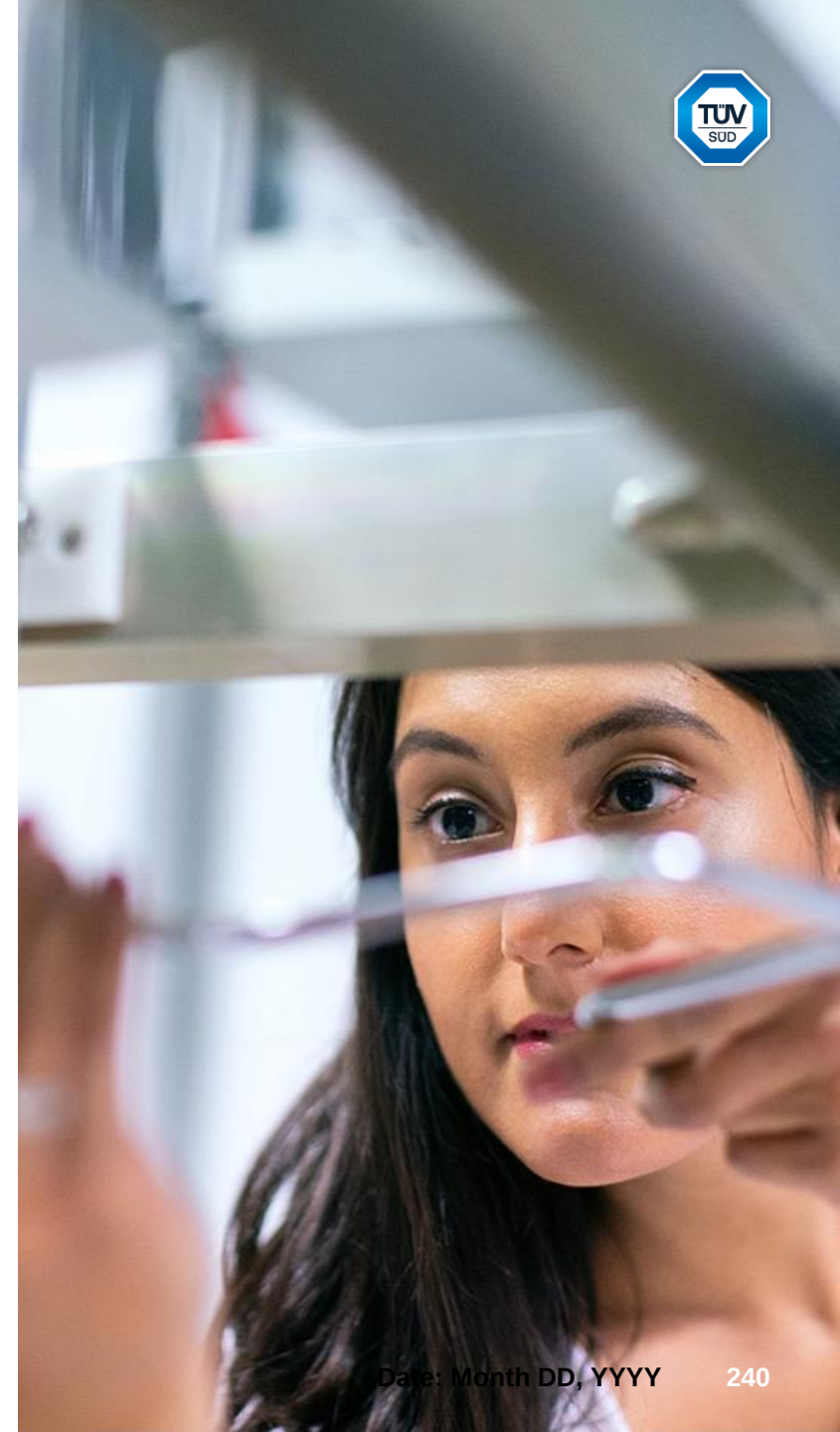
- Bow ties workshops shall be attended by multi-disciplinary team
- Draft bow ties shall be developed prior to workshop and shall be circulated for review;
- Bow Tie chairman shall be fully aware of the project development;
- Bow Tie scribe shall be familiar with the Bow Tie software;



# Summary

What we have learned in the module

- Bow-Tie Definitions
- WHAT IS A BARRIER?
- WHAT IS A VALID BARRIER?
- Steps to describe a barrier



# Exercise 8 - Questions



Q1) What are the steps of bowtie Methodology ?

Q2) What is a barrier ?

Q3) What is A valid Barrier?

# Reference List



| Source*                                                         |
|-----------------------------------------------------------------|
| <u>Regulation (EU) 2017/745</u>                                 |
| CCPS Guidelines (Centre for Chemical Process Safety)            |
| OSHA Process Safety Management (PSM) Standard (29 CFR 1910.119) |
| ANSI/ISA-84.00.01 - Functional Safety                           |
| IEC 60812                                                       |
| IEC 61508                                                       |
| IEC 61511                                                       |
| IEC 61882                                                       |
| ISO 31000 - Risk Management - Guidelines                        |
| ISO 31010- Risk Management - Risk Assessment Techniques         |





# Note



# Any Question?



**Follow us on:**



[tuvsud.com](https://tuvsud.com)  
[info@tuvsud.com](mailto:info@tuvsud.com)

# Thank You!



**TUV SUD MIDDLE EAST LLC –  
Headoffice Branch**

ICAD III, Mussafah, Abu Dhabi,  
UAE  
Email: [Training.ME@tuvsud.com](mailto:Training.ME@tuvsud.com)  
Tel: + 971 2 6767600

**TUV SUD MIDDLE EAST LLC –  
Dubai Branch**

Business Bay, Dubai , UAE  
Email: [Training.ME@tuvsud.com](mailto:Training.ME@tuvsud.com)  
Tel: +971 4 447 3113